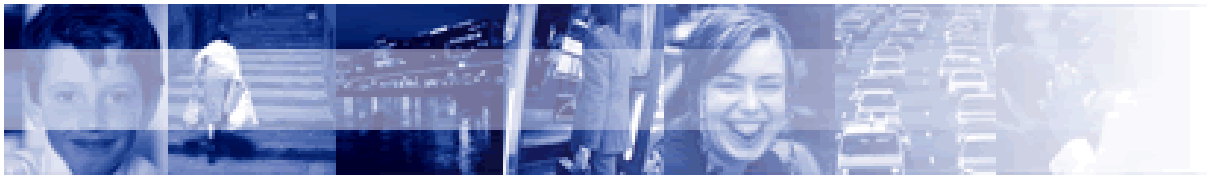
PRISE
privacy • security

Security Research

PASR

Preparatory Action on the enhancement of the European industrial potential in the field of Security research



Grant Agreement no. 108600
Supporting activity acronym: PRISE

Activity full name:
Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies

Activity type: Supporting Activity

Annexes to D 5.7 Spanish report - Interview meeting about security technologies and privacy

Start date of Activity: 1 February 2006 Duration: 28 month

Author(s): Vincenzo Pavone, CSIC Unit of Comparative Policy and Politics

Supporting Activity Co-ordinator
Johann Čas,
Institute of Technology Assessment,
Austrian Academy of Sciences
Strohgasse 45, A-1030 Vienna, Austria
jcas@oeaw.ac.at
www.oeaw.ac.at/ita

Partners

Institute of Technology Assessment,
Vienna, Austria
Contact: Johann Čas
jcas@oeaw.ac.at
www.oeaw.ac.at/ita

The Danish Board of Technology,
Copenhagen, Denmark
Contact: Lars Klüver
LK@Tekno.dk
www.tekno.dk

The Norwegian Board of Technology,
Oslo, Norway
Contact: Christine Hafskjold
christine.hafskjold@teknologiradet.no
www.teknologiradet.no

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,
Kiel, Germany
Contact: Marit Hansen
LD10@datenschutzzentrum.de
www.datenschutzzentrum.de

ANNEXES

(In Spanish)

ANNEX I

Material sent out to the participants:

1) Letter of invitation

Estimada Sr./ Sra:

Tal como quedamos telefónicamente, me pongo en contacto con usted para enviarle el documento sobre el tema que se va a tratar en la reunión de grupo, que como verá, se trata de las nuevas tecnologías aplicadas a la seguridad.

Este documento es una presentación de casos con los que se pretende familiarizar al ciudadano con las diferentes tecnologías de seguridad y las formas en que podrán aplicarse a la vida cotidiana en un futuro próximo.

Se trataría simplemente de que cada uno de su opinión sobre temas, como los que aparecen el los 'papeles' que le envío.

La reunión en la que usted participará se realizará:

Día:
Hora:
Lugar:

Atentamente,

2) SCENARIO

APIS

Acciones preparatorias para la mejora del potencial industrial europeo en el terreno de la investigación sobre seguridad

Acuerdo de subvención nº 108600
Acrónimo de la actividad complementaria: PRISE

Nombre completo de la actividad:
Desarrollo de una investigación sobre seguridad y tecnología que refuerce la privacidad: un planteamiento participativo para idear principios aceptables y aceptados para los sectores y las políticas de seguridad europeos

Tipo de actividad: actividad complementaria

D 4.1 Casos

Fecha prevista de entrega:
Fecha real de entrega:

Inicio de la actividad: 1 de febrero de 2006 Duración: 28 meses

Autor(es):
Christine Hafskjold, Comisión Noruega de Tecnología

Coordinador de la actividad de apoyo

Johann Čas,
Instituto de Evaluación Tecnológica,
Academia Austriaca de las Ciencias
Strohgasse 45, A-1030 Viena, Austria
jcas@oeaw.ac.at
www.oeaw.ac.at/ita

Socios

Instituto de Evaluación Tecnológica
Viena, Austria
Contacto: Johann Čas
jcas@oeaw.ac.at
www.oeaw.ac.at/ita

Comisión Danesa de Tecnología,
Copenhage, Dinamarca
Contacto: Lars Klüver
LK@Tekno.dk
www.tekno.dk

Comisión Noruega de Tecnología,
Oslo, Noruega
Contacto: Christine Hafskjold
christine.hafskjold@teknologiradet.no
www.teknologiradet.no

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,
Kiel, Alemania
Contacto: Marit Hansen
LD10@datenschutzzentrum.de
www.datenschutzzentrum.de

Prefacio

El proyecto **PRISE** aspira a contribuir a un futuro seguro para la Unión Europea que guarde coherencia con los derechos civiles de los ciudadanos europeos – en especial la privacidad - y sus preferencias.

El proyecto:

- Elaborará criterios y directrices para una investigación sobre seguridad y un desarrollo tecnológico que respeten la privacidad.
- Transformará los resultados en casos que presenten aplicaciones de tecnologías de seguridad y medidas que respeten los derechos civiles y la privacidad en distintos grados.
- Pondrá a prueba estos casos en una serie de procedimientos participativos de evaluación tecnológica en diferentes Estados europeos, lo cual ofrecerá un indicativo corroborado de la percepción pública y las preferencias ciudadanas.
- Elaborará una serie de criterios y directrices con la participación directa de proveedores de tecnologías de seguridad, usuarios y destinatarios privados y públicos, instituciones y organismos que desarrollan políticas y normativas, así como organizaciones que representen intereses enfrentados potenciales y reales.
- Distribuirá los resultados entre actores relevantes para el desarrollo de tecnologías y políticas.

Este documento es una presentación de los casos desarrollados en el *Conjunto de Trabajo 4*. Antes de ser mostrados a los grupos de ciudadanos de a pie en diferentes Estados europeos, los casos serán traducidos a su idioma nativo. Los casos pretenden familiarizar al ciudadano corriente con las diferentes tecnologías de seguridad y las formas en que podrán aplicarse a la vida cotidiana en un futuro próximo. Tratamos de abordar distintos planteamientos a las tecnologías, tanto desde el punto de vista del usuario como en la sociedad.

Las descripciones técnicas recogidas en este documento son una adaptación de *D 2.2 Análisis de las Tecnologías de Seguridad*.

El proyecto PRISE desea mostrar su agradecimiento al grupo de expertos que nos ha ayudado a desarrollar los casos:

Asle Fossberg, Servicio de Informática y Material de la Policía Nacional
Marit Gjerde, Colegio Universitario de la Policía Noruega
Nina Græger, Instituto Noruego de Asuntos Internacionales
Ove Skåra, Cuerpo Noruego de Inspectores de Datos
Thomas Olsen, Centro Noruego de Investigación Informática y Legal

También nos gustaría dar las gracias a Jordi Mas, subdirector de la Fundació Catalana per a la Recerca i la Innovació, que ha tenido la amabilidad de aportar sus reacciones sobre los casos a lo largo del proceso.

Introducción

Este documento presenta algunos casos que demuestran cómo pueden utilizarse en un futuro próximo las tecnologías y la vigilancia de seguridad en situaciones cotidianas.

¿Qué es la tecnología de seguridad?

Seguridad puede definirse como la ausencia de peligro, es decir, una situación en la que el estado de las cosas deseado no se ve amenazado o perturbado en ningún sentido. En el contexto del proyecto **PRISE**, la seguridad se entiende como seguridad de la sociedad o, más concretamente, de los ciudadanos que constituyen la sociedad.

El término *tecnología de seguridad* puede abarcar desde un sistema de alarma privado y la protección antivirus para PC a los sistemas de control fronterizo y la cooperación policial internacional. En nuestros ejemplos nos centramos principalmente en tecnologías o medios (sistemas, legislación, etc.) destinados a mejorar la seguridad de la sociedad ante las amenazas de individuos o grupos de individuos (no de Estados). Esto comprende la lucha contra el delito, las actividades antiterroristas, el control fronterizo, etc.

En el texto sobre los casos presentamos algunos datos sobre las diferentes tecnologías para una mejor comprensión de cómo funcionan hoy y de su potencial para el futuro.

¿Qué es privacidad?

La privacidad suele asociarse con la protección de la integridad, la autonomía y la vida privada del individuo. Básicamente consiste en el derecho de la gente a elegir cómo quiere vivir su vida y qué aspectos quiere mantener en privado. La privacidad se considera un derecho humano básico, y la primera regulación de la misma es el artículo 12º de la Declaración Universal de los Derechos Humanos.

Lo que dificulta la protección de la privacidad es el hecho de que casi siempre compite con otros bienes de la sociedad, como la movilidad, la eficiencia, la seguridad o la comodidad. Por ejemplo: aunque sepamos que llevar un teléfono móvil encendido hace posible nuestra localización, ¡a la mayoría de nosotros ni se nos pasa por la cabeza dejar el teléfono en casa! Y casi todo el mundo prefiere llevar un identificador por radiofrecuencia en el coche que hacer cola para pagar en efectivo (anónimo) cuando viaja por una vía de peaje.

Las investigaciones indican que a mucha gente no le preocupan las tecnologías que invaden su privacidad porque cree que no tiene nada que ocultar. Los expertos temen que esto desemboque en una pérdida de la privacidad para la sociedad que sea difícil de recuperar una vez desaparecida. E incluso el ciudadano más respetuoso con la ley puede encontrarse en una situación en la que no querría ser visto o localizado.

En lo relativo a las tecnologías de seguridad y vigilancia, sus detractores afirman que muchas de las medidas que se aplican no son adecuadas para combatir el terrorismo, sino únicamente para convencer a la ciudadanía de que “se está haciendo algo”. Esto se debe a que las medidas pueden burlarse o a que es demasiado improbable que la amenaza que abordan justifique las acciones emprendidas contra ella. Un ejemplo de

esto muy utilizado es la prohibición de las tarjetas telefónicas anónimas en numerosos países. Los detractores de esta prohibición aducen que sólo frena a gente corriente a la que le gustaría permanecer en el anonimato; los delincuentes tienen maneras de eludirla registrándose con una identidad falsa o utilizando teléfonos móviles robados.

Algunas iniciativas antiterroristas, sobre todo en Estados Unidos, infringen la privacidad, como la escucha de llamadas telefónicas, la inspección de las comunicaciones electrónicas sin orden judicial o el análisis de una persona basándose en datos recabados de distintas fuentes sin informar al individuo en cuestión.

Un principio importante de la privacidad es que debería informarse a una persona cuando sus datos personales sean almacenados y procesados, y de que es posible tener acceso a dichos datos y verificar que son correctos. Sólo deberían recabarse y almacenarse datos personales si es realmente necesario, y deberían borrarse cuando ya no se precisen para su propósito original.

¿Qué opina sobre las tecnologías de seguridad?
Casos para estimular el debate

En la siguiente sección presentaremos las historias de dos personas: Carla y Peter. Les seguiremos en sus encuentros con diferentes tecnologías y medios de seguridad, y compartiremos sus pensamientos e ideas sobre estas cuestiones. Para crear unos casos generales, hemos evitado el uso de países, ciudades o aeropuertos concretos como ejemplo. Por el contrario, hemos tratado de demostrar cómo los diferentes países – y las autoridades responsables de la seguridad - han elegido distintos planteamientos para aplicar la tecnología de seguridad. Los casos acontecen en algún momento del futuro para exponer el uso de algunas tecnologías o legislaciones de seguridad que todavía no se han adoptado.

Esperamos que estas historias les inviten a reflexionar sobre la seguridad y la privacidad, y sobre cuál es su opinión acerca de estos dos valores.

Carla tiene 62 años. Ha trabajado toda su vida de profesora, pero ahora se está planteando la jubilación anticipada. ¡Últimamente es todo tan técnico! Y los niños parecen más escandalosos que antes. Tal vez se esté haciendo mayor. Sin embargo, esta semana no se preocupará por eso. Estamos a comienzos de las vacaciones de verano y visitará a su hijo, que vive en un país vecino.

Carla se monta en el metro para ir a la estación central de trenes. Ha "cargado" su *billete universal* y lo utiliza para pagar su trayecto sosteniéndolo frente al lector situado en la barrera. El billete es una tarjeta de plástico que contiene un pequeño chip. Este chip lleva un recuento de los viajes que ha almacenado en su tarjeta. Carla ha elegido lo que se conoce como billete anónimo. Sabe que esto significa que perdería el dinero en caso de extraviar el billete, y además le supone una molestia adicional porque tiene que llevar otra tarjeta. Por supuesto, el *billete universal* corriente está incorporado a la *unidad móvil* de su propietario. Sólo debe llevar la unidad encima o en el bolso y verificarla con su huella dactilar cuando cruce la barrera.

Carla no puede evitarlo: el uso de la huella dactilar para identificarse le resulta desagradable. Es consciente de

que a los jóvenes de hoy en día no parece molestarles en absoluto, pero para ella siempre estará asociado con delincuentes y detenciones. “Ya es bastante malo el tener que dejar tu huella dactilar y mostrar el DNI cuando quieres viajar al extranjero”, opina Carla. ¡Sin duda no quiere hacerlo con más frecuencia de lo que ya lo hace!

Biometría

La tecnología biométrica identifica automáticamente a los individuos utilizando sus características biológicas o conductuales. La biometría puede utilizarse para controlar el acceso a localizaciones físicas o información (ordenadores, documentos). La biometría de uso más habitual son las huellas dactilares y las características faciales.

El proceso de cotejar la biometría de una persona con una plantilla almacenada previamente se conoce como comparación. La comparación da lugar a una puntuación. La aceptación o el rechazo de una persona se basa en si dicha puntuación supera un determinado límite.

En la mayoría de los casos, la imagen biométrica se almacena en forma de *plantilla*, que es una representación digital de la biometría. La plantilla se crea utilizando un algoritmo. Por razones de privacidad, se recomienda almacenar sólo la plantilla y descartar la imagen original. Sin embargo, en los sistemas policiales, como los pasaportes biométricos y los sistemas de reconocimiento facial, con frecuencia se conserva la imagen original.

Podemos distinguir entre *identificación*, que consiste en descubrir quién es una persona comparando su muestra con todas las plantillas almacenadas en un sistema, y *acreditación*, donde la persona de la muestra es comparada con su plantilla guardada para verificar que es quien dice ser.

Un desafío de los sistemas biométricos es encontrar el equilibrio adecuado entre el Índice de Aceptación Falsa (IAF) y el Índice de Rechazo Falso (IRF). *Aceptación falsa* (o *falso positivo*) es cuando un sistema identifica incorrectamente a un individuo. Cuando el sistema no identifica a un individuo registrado, estamos ante un *falso rechazo* (o *falso negativo*).

Una de las grandes ventajas de la biometría es que está muy vinculada a una persona. La acreditación biométrica ofrece un mejor control de acceso, y la usurpación de la identidad es mucho más compleja cuando los datos personales están vinculados exclusivamente a la persona correcta. Pero éste es también el mayor lastre de los sistemas biométricos. Una vez que una serie de datos biométricos se ha visto comprometida, lo está para siempre.

Peter tiene 32 años. Trabaja de comercial para un concesionario de coches. Esta mañana se levantará temprano para asistir a una feria de automóviles celebrada en Europa Central. Sale de la cama, se da una ducha rápida, coge la bolsa, sube al coche y se dirige al aeropuerto. Llega tarde, como siempre, pero al haberse registrado en *facturación rápida* no debería tener problemas. La facturación rápida te ahorra el fastidio que conlleva la facturación en la que los pasajeros son cotejados con el perfil de delincuentes, se verifican los pasaportes y, por supuesto, se realizan los rigurosos controles de seguridad. Con la facturación rápida te someten a un exhaustivo proceso de registro una sola vez y permites que el aeropuerto almacene todos tus datos. A cambio, puedes eludir la facturación ordinaria y acreditarte sólo a la entrada.

Peter piensa en su compañero que, según él, tiene una fijación con la privacidad. Afirma que existe demasiada vigilancia en la sociedad actual, ¡y ahora ni siquiera acepta *cookies* en su ordenador! ¡Incluso ha desinstalado la barra de herramientas de Google, algo que no hace nadie! Si fuese cierto que los organismos estadounidenses utilizan esos datos para trazar redes y buscar perfiles sospechosos, indudablemente sería de dominio público. Ahora debe de llevar un par de horas levantado y ya está haciendo la cola de facturación y seguridad. Bueno, ¡él se lo ha buscado! Peter espera pasar el control de seguridad a tiempo para poder repasar la presentación una última vez antes de embarcar.

- o -

Carla llega a la estación central. Como en el metro, hay cámaras por todas partes. Pantallas y altavoces colgados en la pared repiten advertencias de seguridad hasta que ya nadie les presta atención. “No descuiden su equipaje”, “Su imagen será cotejada con la base de datos de terroristas conocidos”. Hace años se mantuvo un debate sobre esta última. Muchos países no indican mediante carteles que capturan imágenes y las comparan con distintas bases de datos, y se propuso que tampoco tenían por qué hacerlo aquí. Pero el Gobierno dejó muy claro el principio de que la gente debería saber cuándo y dónde está siendo controlada. “Eso es especialmente importante cuando no tienes forma de darte cuenta tú solo. Ya no hay forma de saber si te están haciendo una foto”, reflexiona Carla. Ha oído que hay países en los que también controlan el correo electrónico y las conversaciones telefónicas de la gente en busca de palabras y frases sospechosas, ¡pero seguro que son sólo rumores!

A Carla le da vueltas la cabeza con el ruido y se dirige a la *zona silenciosa*. Tiene que mostrar su carné de identidad para acceder a ella, pero una vez dentro, se relaja. “¡No hay cámaras, teléfonos móviles, zona inalámbrica o avisos ruidosos! Realmente debería haber más zonas sin tecnología como éstas”, opina Carla.

No es que no esté acostumbrada a las cámaras. Al fin y al cabo, las ha tenido a su alrededor gran parte de su vida adulta, ¿pero no parecen más entrometidas últimamente? Después de que empezaran a utilizarse programas de reconocimiento facial y de patrones, parece sentirse más observada y evaluada que antes. “¿Estareé haciendo un gesto como el de un terrorista?”. ¡Imaginen lo embarazoso que sería hacer algo que pudiera provocar su detención y registro por parte de la policía antiterrorista! Para ser justos, en realidad nunca le han dado el alto, pero no puede evitar pensar en ello cuando hay cámaras a su alrededor.

Y, como la mayoría de la gente, conoce a una persona que ha sido acusada de presunto terrorista. Cuando la tecnología se encontraba en sus primeros estadios, había muchos problemas con el programa de reconocimiento facial. Y como los políticos querían evitar el escándalo que supondría que algún integrante de la lista de los más buscados engañara al sistema, el resultado fue una gran cantidad de los denominados *falsos positivos*.

Un compañero suyo, cuyos padres son de Irán, fue confundido con un terrorista. A él le pareció muy humillante, y Carla lo entiende. Como decía su amigo: “Cuando has sido detenido por la policía antiterrorista, vestida con sus chalecos antibalas, y tienes mi aspecto, la gente te mira distinto, aunque te dejen marchar con una disculpa”. Carla sabe que, después de aquello, su compañero se mantuvo alejado de las zonas con muchas cámaras durante un tiempo, sobre todo cuando iba acompañado de sus hijos.

Últimamente, cada vez más gente cuestiona la legitimidad y la eficiencia de las cámaras. En algunas zonas de la ciudad están realizando pruebas en las que, en lugar de cámaras de vigilancia, instalan una iluminación mejor y más intensa, ¡al parecer con buenos resultados!

- o -

Como trabaja en un concesionario, Peter siempre lleva un coche último modelo.

Circuito Cerrado de Televisión (CCTV)

La vigilancia por CCTV mediante *cámaras activas* es cuando un operador observa el monitor y puede controlar la cámara (girar, zoom) para seguir a un individuo o una situación que se está desarrollando. Las cámaras activas pueden utilizarse con programas automatizados de vigilancia visual que emplean algoritmos para detectar movimientos sospechosos o identificar a personas

comparando su imagen con una referencia en una base de datos.

Cámaras pasivas: estas cámaras registran lo que ocurre en un lugar concreto (por ejemplo, un quiosco) en una cinta. Dicha cinta es visionada sólo si se produce un incidente, como un robo, una pelea, etc.

Aunque los primeros sistemas de CCTV eran analógicos, las versiones digitales son cada vez más comunes. La búsqueda por imágenes digitales puede ahorrar tiempo en la localización de acontecimientos específicos o el seguimiento de sospechosos utilizando una base de datos existente, pero el hecho de que dichas imágenes también puedan ser manipuladas con más facilidad podría ser motivo de preocupación.

Reconocimiento facial automático

Los sistemas de reconocimiento facial automático son sistemas en los que se captura automáticamente la imagen de una persona y se compara con una base de datos para su identificación o acreditación. La identificación de una persona aleatoria basada en esta técnica requeriría una base de datos extremadamente grande y una capacidad de procesamiento superior a la que es factible hoy en día. Por tanto, esos sistemas suelen utilizarse para verificar que una persona no figura en una lista de, por ejemplo, delincuentes o terroristas conocidos.

Reconocimiento Automático de Números de Matrícula (RANM)

Los sistemas de RANM leen los números de matrícula captados por un CCTV y los comparan con una base de datos. Los sistemas de reconocimiento de matrículas se utilizan en varios países. En su mayoría guardan relación con el paso por peajes o radares de velocidad, pero también se emplean para identificar vehículos robados.

El que tiene ahora incorpora las tecnologías más recientes: conexión Galileo por satélite con sistema de navegación, llamada automática de emergencia a través del sistema eCall y una serie de sistemas de seguridad para el automóvil. Peter ni siquiera está seguro de para qué sirven todos. Actualmente, el sistema eCall viene de serie en todos los automóviles nuevos, y en principio llama al número de urgencias de forma automática si el coche sufre un accidente. Al estar conectado al sistema Galileo, almacena la posición exacta del coche.

En los últimos años también ha habido propuestas de utilizar la tecnología con otros fines. Tras un intento de atentado en Berlín, los terroristas robaron un coche y huyeron por Alemania. Luego resultó que el sistema también podía utilizarse para realizar un seguimiento del coche, ¡e incluso detenerlo! El automóvil era un modelo caro con la última tecnología antirrobo y, de hecho, podía inmovilizarse a distancia vía satélite. Los terroristas fueron arrestados y, después de esto, los Estados miembro de la UE acordaron que los sistemas podían ser utilizados por la policía para controlar a delincuentes y presuntos terroristas.

Después de un informe de investigación sobre cuántas vidas podrían salvarse si los límites de velocidad fueran respetados por los motoristas, se propuso que los sistemas de seguridad de los vehículos debían integrar un módulo que pudiera verificar el límite de velocidad en un tramo determinado de carretera y compararlo con el velocímetro. La idea original era que un chip incorporado al motor garantizara que ningún coche superaba el límite de velocidad, pero fue recibida con fuertes protestas, tanto del sector automovilístico como de las asociaciones de propietarios de coches. Por el momento, el sistema está configurado de modo que, cada vez que un coche rebasa el límite permitido, se realiza una llamada al registro central de multas, y ésta se deduce automáticamente de la cuenta bancaria del propietario del automóvil.

Peter pisa el acelerador. No todos los tramos de carretera han sido actualizados en el sistema, y se ha descargado a su sistema de navegación un resumen general de los que sí lo están. Recibe una alerta cada vez que pasa junto a una señal vinculada al sistema, lo cual significa que “debe”

respetar el límite de velocidad. “Es positivo que la vigilancia también funcione en el sentido opuesto”, opina Peter.

Peter llega al aeropuerto. El número de matrícula de su coche ya figura en el sistema, y su coche es registrado automáticamente cuando entra en el aparcamiento.

Tecnología de localización

Es posible calcular la posición aproximada del equipo móvil del usuario utilizando coordinadas conocidas o, por ejemplo, estaciones base de GSM.

Para un posicionamiento más preciso, se utilizan sistemas basados en conexiones vía satélite:

GPS es la abreviatura de *Global Positioning System* [Sistema de Posicionamiento Global], un sistema internacional de navegación por satélite constituido por 24 satélites que giran alrededor de la Tierra. Utilizando tres satélites, el GPS puede calcular la longitud y latitud del receptor basándose en el punto en que se cruzan las tres esferas. Mediante el uso de cuatro satélites, el GPS también puede determinar la altitud.

Galileo será una red global de 30 satélites que ofrecerán información precisa sobre tiempos y situación a usuarios que circulen por tierra o aire. Se prevé que esté plenamente operativo en 2010. Será más exacto que el sistema GPS, y tendrá una mayor penetración.

eCall

El dispositivo eCall contiene sensores que se activan tras un accidente. El sistema llama al número de emergencias y transmite información sobre el accidente, incluyendo la hora, la situación exacta, la dirección y la identificación del coche.

El dispositivo no estará conectado permanentemente a una red de comunicaciones móvil. Sólo lo hará cuando haya sido activado. Sin embargo, preocupa que esto pueda cambiar, y también la transmisión de otros datos (por ejemplo, para las compañías aseguradoras) y un posible acceso no autorizado a las bases de datos en las que se almacena la información de eCall. Desde septiembre de 2009, todos los coches nuevos de los países participantes irán equipados con eCall.

Es la misma tecnología que se está utilizando en las ciudades para identificar vehículos robados. Peter en realidad creía que ese sistema sería innecesario después de que el eCall se conectara a Galileo, pero, al parecer, las bandas más organizadas saben cómo desactivar el sistema. Y sabe que algunos países exigen incluso que el conductor pueda deshabilitar él mismo el sistema eCall. ¡Ese tipo de requisitos siempre complican las cosas al sector automovilístico! ¿Y por qué los delincuentes siempre parecen ir un paso por delante de la tecnología?

Desviación de funciones

Los sistemas de bases de datos son vulnerables a la denominada desviación de funciones, es decir, la utilización de datos con un fin distinto del original. Un ejemplo de esa desviación de funciones se observó cuando la base de datos noruega de buscadores de asilo – que también contiene información biométrica como las huellas dactilares - quedó abierta a la policía para las investigaciones criminales. La intención original de la base de datos era ayudar a determinar la identidad de los buscadores de asilo.

Peter aparca, sale del coche, se dirige a la terminal, y luego a la entrada de facturación rápida. Coloca el dedo en el sensor y mira directamente a la cámara. Parpadea una luz verde y se abre la puerta.

Aunque los sensores son mucho mejores que antes, algunos todavía tienen problemas para utilizar la toma de huellas: como le pasó a su abuelo, por ejemplo. Aunque es un hombre de 80 años que está muy en forma, se está aislando cada vez más. Últimamente tienes que utilizar la huella dactilar con el DNI en todas partes, y le incomodan las molestias que se producen cuando el sensor no puede leerlas, así que se queda en casa la mayoría del tiempo.

Peter a veces va a la biblioteca a cogerle libros *de verdad*. Le divierte pensar en cómo será su perfil de la biblioteca. Si alguna vez lo analizan cuando busquen a individuos sospechosos, el servicio de espionaje quizá se pregunte por qué un hombre de treinta y tantos años toma prestados libros como *Dating for seniors* [Citas para ancianos] y *Our*

friends the birds [Nuestros amigos los pájaros].

Hace unos años, justo después de que se frustrara un gran atentado terrorista en EE UU, se propuso que debía permitirse a los organismos de seguridad investigar todas las bases de datos posibles. Y no se limitaba a los presuntos delincuentes o terroristas. Pretendían analizar todo el material de las bases de datos bibliotecarias, los patrones de consumo de electricidad y gas, el tráfico de teléfono e Internet, la información sobre viajes y los hábitos de compras. Mediante la búsqueda de patrones sospechosos querían identificar a posibles terroristas.

Su compañero Alex estaba indignado, y Peter había intentado discutir con él: sin duda no pedirían esto a menos que tuvieran motivos. Lógicamente, las autoridades deberían hacer cualquier cosa que estuviese en su mano para atrapar a los terroristas. Alex no estaba convencido, y alegaba que al menos podrían realizar el análisis con datos anónimos: "Si encuentran algo sospechoso, pueden obtener una orden judicial para que se revele la identidad. ¡No existe ningún motivo legítimo por el que deban saberlo todo acerca de todo el mundo!".

A Peter en realidad no le interesaba demasiado debatir más el tema, pero su colega no dejaba de hablar de ello en cada descanso para comer, y él acabó firmando una petición contra la propuesta. "Pero la verdad es que no le encuentro el sentido", afirmó Peter. "Esto sólo es un problema para los que tienen algo que ocultar". Por otro lado, se sorprendió preguntándose si habría quedado registrado en algún sitio que había firmado la petición…

Conocimiento Total de Información (CTI)

Conocimiento Total de Información (CTI) era un programa del Organismo de Proyectos de Investigación Avanzada de Defensa de EE UU (DARPA, por sus siglas en inglés). El programa CTI contenía tres categorías de herramientas: traducción de idiomas, búsqueda de datos y reconocimiento de patrones, y herramientas de apoyo avanzadas para colaboración y decisión.

El objetivo del CTI era predecir atentados terroristas antes de que se produjeran. El sistema debía investigar bases de datos privadas y públicas, así como Internet, en busca de transacciones que pudieran estar relacionadas con un atentado. El Congreso de EE UU canceló la financiación del CTI en septiembre de 2003, pero muchos programas del sistema han continuado con nombres diferentes.

Carla se sienta un rato en la zona silenciosa a leer un libro, y luego se dirige hacia la puerta de seguridad.

La puerta de seguridad de la terminal internacional de trenes nació a raíz de una mayor demanda de control, no sólo en los aeropuertos, sino en otros lugares en los que se congrega mucha gente. Carla sabe que en algunos países incluso se realizan controles de seguridad a la entrada de los centros comerciales y de los estadios deportivos. Hace un par de años, se descubrió a un terrorista en un centro comercial situado cerca de donde vive su hijo. Al parecer, acababan de empezar a utilizar un equipo de escáner a la entrada y el terrorista no lo sabía. Aun así, se alegra de que en su país no hayan ido tan lejos. Hasta la fecha, sólo las terminales aéreas y ferroviarias incluyen seguridad con escáner para pasajeros.

A Carla no le preocupan los centros comerciales; al fin y al cabo, no se ha proferido ninguna amenaza contra su país, que ella sepa. Pero ha visto estadísticas que demuestran que cada vez más gente está volviendo a comprar en los establecimientos más pequeños del centro de los pueblos y las ciudades, y que las grandes superficies afirman estar perdiendo ingresos porque no se les permite colocar equipos de escaneo como las *máquinas al desnudo.*

Carla saca el pasaporte y se acerca al escáner de iris. Sabe que algunos países todavía utilizan las huellas dactilares en los DNI y pasaportes, pero ella considera que el iris es más seguro. El

lector compara su iris con la plantilla almacenada en su pasaporte. Antes le preocupaba, pero su hijo, que trabaja en el sector de las tecnologías de la información, le ha garantizado que ahora es totalmente seguro. "La codificación original del primer pasaporte era bastante mala", afirma su hijo, "pero con la que se utiliza ahora, ¡un superordenador tendría que invertir miles de años para descifrarla! Además, en los primeros pasaportes guardaban la imagen real del rostro y las huellas dactilares o el iris. Ahora sólo almacenan una *plantilla*, una representación digital de la característica más importante del iris y la cara.

Identificación por Radiofrecuencia (IRF)

La IRF es un concepto para la identificación automática utilizando radiofrecuencias. Unos diminutos circuitos incorporados (etiquetas) que contienen información se adjuntan a los documentos o se integran en los productos. Puede utilizarse un *lector* para leer la información de las etiquetas dentro de su alcance.

Las etiquetas de IRF pueden incorporar chips *activos* y *pasivos*. Las etiquetas activas – como los Teletac de las autopistas - contienen una batería y, por tanto, son más grandes que las etiquetas pasivas, pero pueden almacenar más información y funcionar a mayor distancia. Las etiquetas pasivas no incluyen batería, pero obtienen su energía de la señal de radio del lector. Una aplicación típica de las etiquetas pasivas es el nuevo pasaporte europeo. .

La mayoría de las etiquetas se comunican con cualquier lector, pero algunas piden al lector que introduzca una contraseña o aporte otra credencial.

Pasaporte biométrico

Un pasaporte biométrico consiste en el documento real, normalmente en forma de folleto, y un chip diminuto.

El chip contiene datos obligatorios y opcionales. Al margen de eso, incluye una fotografía del usuario como vínculo visual entre el propietario y el pasaporte.

La Organización Internacional de Aviación Civil (OIAC) ha optado por un chip que puede leerse a cierta distancia (como las tarjetas identificadoras sin contacto con el sistema de lectura). La OIAC ha elegido el *rostro* como biometría principal para utilizarla en los pasaportes. El *dedo* y el *iris* se recomiendan como biometrías secundarias. La UE se ha decidido sólo por el dedo como biometría secundaria.

Los pasaportes biométricos han suscitado muchos debates, sobre todo relacionados con la seguridad de la información biométrica. Existe el temor de que pueda robarse la información leyéndola a distancia sin el conocimiento del propietario o interceptándola cuando se está transmitiendo.

Para abordar estas preocupaciones se ha desarrollado un esquema de "control de acceso básico" (CAB). Según el CAB, el sistema de inspección utiliza una "clave" derivada de datos numéricos que contiene la zona legible de la Máquina (el código de barras) para "desbloquear" el chip, de modo que el sistema pueda leerlo. El CAB ha sido criticado por no ser lo bastante fiable, y algunos expertos en seguridad han logrado averiguar el código cifrado en un breve periodo de tiempo.

Aunque alguien lo descodificara, no podría recrear el rostro o el iris para hacerse pasar por el propietario del pasaporte".

También le han asegurado que el lector sólo almacena la plantilla de su iris el tiempo suficiente para compararlo con el de su tarjeta, y que no se guarda en una base de datos central. No tiene tan claro qué sucede cuando se verifica su pasaporte en otra frontera. ¿También se borran los datos después de cotejarlos?

Carla recuerda que hace unos años estalló un escándalo en torno a una base de datos central de huellas dactilares. ¿Fue en EE UU? Un empleado robó gran cantidad de huellas y las vendió a delincuentes internacionales. Miles de personas vieron cómo les era usurpada su personalidad y experimentaron toda clase de problemas, desde aparecer en la "lista negra" de los aeropuertos a que les vaciaran las cuentas bancarias. Fue especialmente difícil porque el gobierno tardó mucho tiempo en reconocer que había perdido los datos. ¡Y, entretanto, nadie se creía que le hubieran robado su identidad o que pudiesen utilizarse las huellas de alguien para hacerlo!

Sin embargo, Carla es más lista. El verano pasado, a un amigo de su hijo le robaron el DNI, justo antes de que él y su familia se fueran de vacaciones. Temía verse obligado a cancelarlo todo por si aparecía en la "lista negra", pero, al parecer, el sistema de información Schengen que se utiliza en numerosos países europeos registra a la gente a la que le han usurpado su identidad. Gracias a esto, él y su familia pudieron viajar tal y como habían planeado, y jamás fue acusado de ser un delincuente o un terrorista, aunque su DNI probablemente fue verificado más exhaustivamente que el de un viajero corriente.

Tras la comprobación de su DNI, Carla debe pasar su equipaje por el escáner, antes de pasar por lo que antes se conocía como la *máquina al desnudo.* Le alivia que la máquina al desnudo nunca llegara a comprarse para los aeropuertos y las terminales ferroviarias internacionales de su país.

Escáner de pasajeros (*Máquinas al desnudo*)

Las tecnologías como los *rayos X por retrodispersión o radiación Terahertz* penetran mejor en los materiales que la óptica. Eso significa que pueden utilizarse para la detección y la obtención de imágenes de artículos ocultos por la ropa.

Una "máquina al desnudo" utiliza este tipo de tecnología para revelar si una persona lleva armas o explosivos ocultos en su cuerpo. Se utilizan diferentes sistemas. Algunos revelan todo lo que hay debajo de la ropa – no sólo pistolas y explosivos -, de ahí su nombre. Este tipo de seguridad aeroportuaria se ha probado en Heathrow (Terminal 4) desde 2004. Otras aplicaciones captan las imágenes de objetos ocultos y las proyectan en un maniquí asexuado.

Las autoridades de seguridad evaluaron distintas máquinas, pero decidieron que era igual de seguro adquirir el modelo en el que los artículos ocultos bajo la ropa se proyectan sobre una imagen neutra de una persona.

A sus 62 años, Carla todavía se avergüenza de su cuerpo, y se alegra de que el joven del acceso de seguridad no pueda verla desnuda. Debe quitarse los zapatos, pero, aparte de eso, no tiene ningún problema y pronto está cómodamente sentada en el tren.

- o -

Peter cruza el vestíbulo del aeropuerto y se dirige hacia el control de seguridad. Por supuesto, incluso los clientes de facturación rápida deben pasar por algún tipo de sistema de seguridad, pero tienen su propio acceso, y todos son profesionales en esto. Nadie en *este* acceso lleva hebillas de metal o es lo bastante aficionado como para guardar calderilla en el bolsillo. Y hace años que los zapatos fabricados para el sector de los negocios no contienen metal. Peter mete barriga y pasa por la *máquina al desnudo*. "¿Por qué siempre tienen la temperatura tan baja en esta sala?", piensa, y se pone colorado al darse cuenta de que una de las guardias de seguridad es una mujer más o menos de su edad.

Retención de datos

Una base de datos se define como una colección organizada de información. Por lo general, se reconoce que cuando pueden recabarse distintos datos sobre alguien, revelan más de esa persona que la información estudiada por separado. Por ello, un principio importante de la privacidad relacionado con las bases de datos que contienen información acerca de las personas es que sólo deberían recabarse los datos necesarios para satisfacer el propósito del sistema, y que deberían borrarse cuando ya no se necesiten.

Últimamente hemos observado una tendencia en la que los gobiernos han pretendido almacenar más información y conectar los sistemas de bases de datos con fines distintos del original, como la seguridad. El tipo de datos a los que más se alude cuando se debate la retención de datos son los relacionados con las tecnologías de la información y las comunicaciones, como los datos del tráfico de teléfonos, móviles e Internet.

La UE ha aprobado una directiva sobre la retención de esos datos. Se almacenarán datos sobre quién, cuándo y dónde se comunica, pero no el contenido de las conversaciones. Los datos pueden guardarse durante un periodo máximo de dos años.

Varios departamentos de EE UU anunciaron en 2005 que habían comprado información personal a los denominados *revendedores de información* por unos 22 millones de euros. Estos negocios recaban y agregan información personal de múltiples fuentes y la ofrecen a sus clientes. Las fuentes pueden ser archivos públicos, datos disponibles públicamente (por ejemplo, en Internet) e información de fuentes privilegiadas como empresas privadas.

Aun así, está encantado de que el aeropuerto utilice la máquina al desnudo *real*. Por alguna razón le parece más segura.

Peter advierte un nuevo elemento de seguridad que no había visto antes. Después de la máquina al desnudo hay una segunda "puerta" por la que se pide a algunos pasajeros que pasen. Recuerda vagamente haber oído algo sobre un nuevo elemento de seguridad que se estaba probando en este aeropuerto. Supuestamente registra características como el calor corporal, el sudor, el ritmo cardiaco, etc., aspectos que puedan ser indicativos de enfermedades como el SARS o la gripe aviar, o de que una persona está nerviosa. Algunos de los sujetos sometidos a la prueba son conducidos a salas de entrevistas cercanas. Se alegra de que no le hayan elegido para la prueba, aunque está sano y tiene la conciencia tranquila. "Pero, ¿por qué tienen que ponerlo en *facturación rápida*? ¿No saben que la gente que la utiliza está ocupada?".

Se dirige hacia la puerta y se sienta. Quizá debería llamar a Yasmin y decirle que va. Ella trabaja para el fabricante al que representa su concesionario, y la conoció en la última feria a la que asistió. Congeniaron al momento, y le gustaría mucho volver a verla. Por otro lado, es reacio a llamarla al móvil. Sabe que el hermano de Yasmin es un elemento muy activo de un grupo de jóvenes de su mezquita, y que Yasmin probablemente figure en alguna lista de vigilancia como parte de la "red" de su hermano. Ojalá hubiese comprado una tarjeta telefónica anónima la última vez que estuvo en Asia. Ya no es legal venderlas en Europa.

Interceptación de las comunicaciones

Pueden utilizarse diferentes aplicaciones para controlar a los ciudadanos y la interacción entre ellos, ya sea por Internet, la red telefónica o áreas definidas. Una forma de interceptación de las comunicaciones a menudo se conoce como *escuchas telefónicas.* Básicamente consiste en instalar un dispositivo de escucha en el recorrido entre dos teléfonos que están participando en una conversación. Se puede pinchar el teléfono del sospechoso o el de las personas con las que se espera que se ponga en contacto.

Una versión ampliada de las escuchas es pinchar de forma más indiscriminada todas las líneas de comunicación (teléfono, móvil e Internet) en busca de conversaciones que puedan resultar de interés. Un ejemplo de esto es la red Echelon, dirigida por una alianza entre EE UU, Reino Unido, Canadá, Australia y Nueva Zelanda. En un principio, el sistema se creó para controlar las comunicaciones de la Unión Soviética y Europa del Este. Pueden analizarse patrones de comunicación y examinar el contenido en busca de palabras clave interesantes.

Peter tampoco quiere utilizar un servicio de Internet. ¿Quién sabe qué registros llevan las redes del aeropuerto? Ni siquiera está seguro de cuáles son las normativas actuales. ¿Tiene la policía acceso directo a este tipo de datos o necesita una orden judicial? De repente, le gustaría haber prestado más atención al debate sobre la privacidad. Sin duda le preguntará a su colega cuando se suba al avión.

La última vez que cenó con Yasmin, ésta le dijo que estaba convencida de ue examinaban su correo electrónico, y le pidió a Peter que utilizara un programa de codificación si quería escribirle. "Un correo no cifrado es como una postal", explicó Yasmin. "Cualquiera que acceda a él puede leerlo. ¿No lo sabías?".

Peter realmente pensaba que le escribiría, pero descubrió que el programa de correo electrónico que utilizan en su trabajo no incorpora codificación, y nunca llegó a instalar

otro. Espera que Yasmin no esté enfadada con él por ignorarla todo este tiempo. “Se lo explicaré cuando nos veamos”, piensa Peter.

Es hora de subir al avión. Peter se acerca al acceso, pone el dedo en el sensor y es uno de los primeros pasajeros en embarcar. Todavía queda mucho espacio para el equipaje de mano. Piensa en su compañero, que probablemente siga haciendo cola en el control de seguridad, antes de reclinarse y cerrar los ojos.

- o -

“Mamá está de camino”, le dice el hijo de Carla a su mujer después de recibir un mensaje en el móvil. “Debería estar aquí en tres horas”. Su madre no lo sabe, pero la nueva unidad móvil que le regalaron por Navidad está conectada a un servicio llamado *Kid-watch*. La tecnología es una nueva versión de los rastreadores que aparecían en las viejas películas de espías, en las que los vigilantes podían ver a sus sospechosos como pequeños puntos en un mapa. La principal diferencia es que, al utilizar la tecnología incorporada de Galileo en la unidad móvil, puede seguir los movimientos de su madre en un mapa, aunque esté en otro país, sentado en el salón.

Tecnologías para la mejora de la privacidad

Las tecnologías que contribuyen directamente a preservar la privacidad se conocen como Tecnologías para reforzar la privacidad (TRP).

La *Anonimización* es una de esas TRP. Hay servicios que permiten la comunicación electrónica anónima a usuarios habituales. Esa tecnología oculta la relación entre el usuario y las huellas que deja a su paso y, por tanto, puede impedir la identificación no deseada. El pago tradicional en efectivo o las tarjetas telefónicas (anónimas) no registradas son un medio que ofrece anonimato.

La *gestión de la identidad* también es una forma de TRP: en algunos casos, no queremos identificarnos y utilizamos un pseudónimo (por ejemplo, en los foros de Internet). Para que sea más difícil cotejar datos, puede ser una buena idea el tener diferentes nombres de usuario (que no revelan la identidad) y contraseñas para distintos fines. Los sistemas de gestión de la identidad ayudan a la gente a realizar un seguimiento de sus diferentes nombres de usuario. En algunos casos, el servicio en cuestión quizá sólo necesite verificar un atributo concreto, como la edad o el límite de crédito. En esos casos, el *proveedor de identidad* (es decir, su banco, proveedor de telecomunicaciones o empresa) puede actuar como tercera parte fiable y garantizar ese atributo sin revelar su identidad.

La *Codificación* consiste en distorsionar el contenido para hacerlo ilegible a los demás. Debido a que todas las comunicaciones electrónicas son vulnerables a la vigilancia o la manipulación, en muchos casos es crucial que la comunicación se realice en líneas codificadas, o que el contenido que se transmite esté cifrado.

Sin embargo, intenta no consultarlo mucho. Le parece que es husmear demasiado en su vida privada, pero ha introducido algunos indicadores que activan alarmas si su madre no se mueve durante periodos largos dentro de la casa, o si no está en ella por la noche. Al fin y al cabo, se está haciendo mayor y no puede cuidarla como cree que debería, ya que vive en otro país. Suena el teléfono: “Hola, soy mamá. Estoy de camino. Debería llegar a la estación en unas tres horas”…

ANNEX II

QUESTIONNAIRE

Cuestionario sobre tecnología de seguridad y privacidad

Bienvenido al cuestionario del proyecto PRISE sobre actitudes hacia la tecnología de seguridad y la privacidad

En este cuestionario se le plantearán una serie de preguntas. *Rodee con un círculo el número situado junto a la respuesta que quiere dar*. Sólo debe indicar *una* respuesta por pregunta, excepto cuando se especifique "puede marcar más de una respuesta a esta pregunta". Si marca la respuesta incorrecta, táchela y rodee con un círculo la adecuada. En caso de duda sobre el significado de las preguntas, estaremos encantados de resolverlas.

Preguntas sobre antecedentes:

1. Sexo

1. Hombre
2. Mujer

2. Edad *(abierta)*

- Edad: _____

3. ¿Número de personas que viven en su casa, usted incluido?

1. 1 persona
2. 2 personas
3. 3 personas
4. 4 personas o más

4. ¿Tiene hijos?

1. Sí
2. No

5. ¿En su casa vive algún niño? ***(puede marcar más de una respuesta a esta pregunta)***

1. No
2. Sí, de 14 años o menos
3. Sí, de más de 14 años

6. ¿Cuál es el nivel educativo máximo que ha alcanzado?

1. Escuela elemental – 7 años de escolarización
2. Escuela intermedia - 8 o 9 años de escolarización
3. Formación profesional (nivel cualificado/formación artesanal)
4. Escuela secundaria (título de bachillerato)
5. Educación superior de corta duración (menos de 3 años de estudio)
6. Educación superior de duración media (3 - 4 años de estudio)
7. Educación superior avanzada (más de 4 años de estudio)

7. Indique su ocupación (*cuadro de texto abierto)*

- Ocupación: _____

8. ¿Vive en una ciudad o en el campo?

1. Zona metropolitana
2. Ciudad de provincias, más de 50.000 habitantes
3. Ciudad de provincias, 20.000 – 50.000 habitantes
4. Ciudad de provincias, 10.000 – 20.000 habitantes
5. Ciudad de provincias, 2.000 – 10.000 habitantes
6. Zona rural, menos de 2.000 habitantes

9. ¿Con qué frecuencia utiliza el teléfono móvil?

1. Al menos una vez al día
2. Al menos una vez a la semana
3. Al menos una vez al mes
4. Menos de una vez al mes
5. Nunca utilizo el teléfono móvil

10. ¿Con qué frecuencia escribe correos electrónicos?

1. Al menos una vez al día, cada día

2. Al menos una vez a la semana
3. Al menos una vez al mes
4. Menos de una vez al mes
5. Nunca escribo correos electrónicos

11. ¿Con qué frecuencia utiliza Internet?

1. Al menos una vez al día, cada día
2. Al menos una vez a la semana
3. Al menos una vez al mes
4. Menos de una vez al mes
5. Nunca utilizo Internet

12. ¿Con qué frecuencia viaja en transporte público?

1. Al menos una vez al día, cada día
2. Al menos una vez a la semana
3. Al menos una vez al mes
4. Menos de una vez al mes
5. Nunca viajo en transporte público

13. ¿Con qué frecuencia viaja en avión? (Un viaje de ida y vuelta cuenta como una vez)

1. Más de 5 veces al año
2. 3-5 veces al año
3. 1-2 veces al año
4. Menos de 1 vez al año
5. Nunca

14. ¿Con qué frecuencia viaja en coche?

1. Al menos una vez al día, cada día
2. Al menos una vez a la semana
3. Al menos una vez al mes
4. Menos de una vez al mes
5. Nunca viajo en coche

Preguntas generales sobre tecnología de seguridad y privacidad

A continuación encontrará varias afirmaciones sobre tecnología de seguridad y privacidad que aparecen en el debate público. ¿En qué medida coincide con estas afirmaciones?

Indique hasta qué punto está de acuerdo con cada afirmación

- Si cree que la afirmación es totalmente correcta, marque 1 "Totalmente de acuerdo"
- Si cree que la afirmación es correcta pero tiene ciertas reservas, marque 2 "Parcialmente de acuerdo"
- Si le resulta imposible valorar si la afirmación es correcta o incorrecta, marque 3 "Ni coincido ni discrepo"
- Si cree que la afirmación es incorrecta pero tiene ciertas reservas, marque 4 "Parcialmente en desacuerdo"
- Si cree que la afirmación es totalmente incorrecta, marque 5 "Totalmente en desacuerdo"

15. "La seguridad de la sociedad depende totalmente del desarrollo y el uso de nuevas tecnologías de seguridad"

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

16. "Muchas tecnologías de seguridad en realidad no mejoran la seguridad, sino que únicamente se aplican para demostrar que se está haciendo algo para combatir el terrorismo"

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

17. "Si no se tiene nada que ocultar, no hay razón para preocuparse por las tecnologías de seguridad que invadan la privacidad"

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo

4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

18. “Cuando se dispone de tecnología de seguridad, lo lógico es hacer uso de ella”

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

19. “La privacidad no debería ser violada sin una sospecha razonable de intención delictiva”

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

20. “Es incómodo ser vigilado, aunque no se tengan intenciones criminales”

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

21. “Es probable que los organismos gubernamentales abusen de las nuevas tecnologías de seguridad”

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

22. “Es probable que los delincuentes abusen de las tecnologías de seguridad”

1. Totalmente de acuerdo
2. Parcialmente de acuerdo

3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

Tecnologías de seguridad

En esta sección se le formularán preguntas sobre su actitud hacia tecnologías de seguridad concretas y su uso. Los cuadros de texto grises ofrecen información breve acerca de las tecnologías sobre las que se pregunta a continuación. Los cuadros contienen cierta información sobre tecnologías que coincide con los cuadros de los casos enviados por anticipado. Para más datos sobre las tecnologías, véanse los casos.

Una parte de estas preguntas sobre tecnología se centra en el uso aceptable de dichas tecnologías, y en la mayoría de los casos será posible dar más de una respuesta.

La otra parte de las preguntas sobre tecnología son afirmaciones concretas. Indique hasta qué punto está de acuerdo con cada afirmación.

Biometría

La tecnología biométrica identifica automáticamente a los individuos utilizando sus características biológicas o conductuales. La biometría puede utilizarse para controlar el acceso a localizaciones físicas o información (ordenadores, documentos). La biometría de uso más habitual son las huellas dactilares y las características faciales.
La imagen biométrica puede almacenarse como la imagen original o en forma de *plantilla* que es una representación digital de la biometría. Por razones de privacidad, se recomienda almacenar sólo la plantilla y descartar la imagen original. Sin embargo, en los sistemas policiales, como los pasaportes biométricos y los sistemas de reconocimiento facial, con frecuencia se conserva la imagen original.
Una de las grandes ventajas de la biometría es que está muy vinculada a una persona. La acreditación biométrica ofrece un mejor control de acceso, y la usurpación de la identidad es mucho más compleja cuando los datos personales están vinculados exclusivamente a la persona correcta. Pero éste es también el mayor lastre de los sistemas biométricos. Una vez que una serie de datos biométricos se ha visto comprometida, lo está para siempre.

Pasaporte biométrico

Un pasaporte biométrico consiste en el documento real y un chip incorporado que contiene datos. El chip puede ser leído por un sistema de lectura.
Los pasaportes biométricos han sido objeto de debate, ya que se teme que la información biométrica del chip pueda ser robada mediante una lectura a distancia sin el conocimiento del propietario o interceptándola cuando se está transmitiendo.
Un desafío de los sistemas biométricos es encontrar el equilibrio adecuado entre el Índice de Aceptación Falsa (IAF) y el Índice de Rechazo Falso (IRF). *Aceptación falsa* (o *falso positivo*) es cuando un sistema identifica incorrectamente a un individuo. Cuando el sistema no identifica a un individuo registrado, estamos ante un *falso rechazo* (o *falso negativo*).

23. ¿Con qué biometría se sentiría cómodo para un control de acceso? (*Puede marcar más de una respuesta a esta pregunta)*

1. Características faciales
2. Huellas dactilares
3. Reconocimiento del iris
4. No me sentiré cómodo utilizando ninguna biometría para un control de acceso
5. No lo sé

24. ¿Dónde es aceptable el uso de la biometría para un control de acceso? (*Puede marcar más de una respuesta a esta pregunta)*

1. Aceptable para los controles de seguridad en bancos
2. Aceptable para la seguridad aeroportuaria
3. Aceptable para los controles de seguridad en tiendas
4. Aceptable para el control fronterizo
5. Aceptable para el control de seguridad en estaciones centrales de autobuses y trenes
6. Aceptable para el control de seguridad en estadios deportivos y otros lugares/acontecimientos de masas
7. Aceptable para el control de seguridad en otros servicios privados no mencionados
8. Nunca es aceptable
9. No lo sé

Afirmaciones concretas sobre la biometría

25. "El almacenamiento de datos biométricos (por ejemplo, las huellas dactilares o las muestras de ADN) de todos los ciudadanos en una base de datos central es un paso aceptable para combatir el delito"

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

26. “El uso del pasaporte biométrico me hace sentir inseguro por el riesgo de que mis datos biométricos sean robados”

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

Circuito Cerrado de Televisión (CCTV)

La vigilancia por CCTV mediante *cámaras activas* es cuando un operador observa el monitor y puede controlar la cámara (girar, zoom) para seguir a un individuo o una situación que se está desarrollando. Las cámaras activas pueden utilizarse con programas automatizados de vigilancia visual que emplean algoritmos para detectar movimientos sospechosos o identificar a personas comparando su imagen con una referencia en una base de datos..
Cámaras pasivas: estas cámaras registran lo que ocurre en un lugar concreto (por ejemplo, un quiosco) en una cinta. Dicha cinta es visionada sólo si se produce un incidente, como un robo, una pelea, etc.

Reconocimiento facial automático

Los sistemas de reconocimiento facial automático son sistemas en los que se captura automáticamente la imagen de una persona y se compara con una base de datos para su identificación o acreditación. Normalmente se utilizan esos sistemas para verificar que una persona no figura en una lista de, por ejemplo, delincuentes o terroristas.
Reconocimiento Automático de Números de Matrícula (RANM)
Los sistemas de RANM leen los números de matrícula captados por un CCTV y los comparan con una base de datos. Los sistemas de reconocimiento de matrículas se utilizan en varios países. En su mayoría guardan relación con el paso por peajes o radares de velocidad, pero también se emplean para identificar vehículos robados.

Escáner de pasajeros (*Máquinas al desnudo*)

Las tecnologías como los *rayos X por retrodispersión o radiación Terahertz* penetran mejor en los materiales que la óptica. Eso significa que pueden utilizarse para la detección y la obtención de imágenes de artículos ocultos por la ropa.
Una “máquina al desnudo” utiliza este tipo de tecnología para revelar si una persona lleva armas o explosivos ocultos en su cuerpo. Se utilizan diferentes sistemas. Algunos revelan todo lo que hay debajo de la ropa – no sólo pistolas y explosivos -, de ahí su nombre. Este tipo de seguridad aeroportuaria se ha probado en Heathrow (Terminal 4) desde 2004. Otras aplicaciones captan las imágenes de objetos ocultos y las proyectan en un maniquí asexuado.

27. ¿Dónde puede aceptar la vigilancia mediante CCTV? (*Puede marcar más de una respuesta a esta pregunta*)

1. En las tiendas
2. En los probadores, para evitar hurtos
3. En estaciones centrales de autobuses y trenes
4. En los bancos
5. En los aeropuertos
6. En estadios deportivos y otros lugares/acontecimientos de masas
7. En todos los espacios públicos
8. Nunca es aceptable
9. No lo sé

28. ¿En general qué opina sobre el número de cámaras de CCTV en espacios públicos?

1. Debería haber más cámaras de CCTV en los espacios públicos
2. El número de cámaras de CCTV en espacios públicos es apropiado
3. Debería haber menos cámaras de CCTV en los espacios públicos
4. No debería haber cámaras de CCTV en los espacios públicos
5. No lo sé

29. ¿Dónde son necesarios para la seguridad los escáneres para personas destinados a la detección de objetos ocultos? (*Puede marcar más de una respuesta a esta pregunta*)

1. En las escuelas
2. En estaciones centrales de autobuses y trenes
3. En aeropuertos
4. En centros comerciales
5. En edificios públicos (por ejemplo, los juzgados)
6. Nunca son necesarios
7. No lo sé

30. ¿Qué tipo de escáneres consideraría aceptables? (*Puede marcar más de una respuesta a esta pregunta*)

1. Un escáner que revele todo lo que oculta la ropa
2. Los escáneres en los que las imágenes y los objetos ocultos se proyecten sobre un maniquí

3. Los escáneres de calor corporal, sudor y ritmo cardiaco
4. Los escáneres para objetos metálicos
5. El escaneo de equipajes por rayos X
6. Los escáneres no son aceptables
7. No lo sé

Afirmaciones concretas sobre CCTV y escáneres para pasajeros

31. “La vigilancia por CCTV me hace sentir más seguro”

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

32. “La vigilancia por CCTV invade mi privacidad”

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

33. “Los escáneres para personas destinados a la detección de objetos ocultos son una herramienta aceptable para prevenir el terrorismo”

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

Tecnología de localización

Es posible calcular la posición aproximada del equipo móvil del usuario utilizando coordinadas conocidas o, por ejemplo, estaciones base de GSM.
Para un posicionamiento más preciso, se utilizan sistemas basados en conexiones vía satélite:

GPS es la abreviatura de *Global Positioning System* [Sistema de Posicionamiento Global], que es el sistema existente. Se prevé que *Galileo* esté plenamente operativo en 2010. Será más exacto que el sistema GPS, y tendrá una mayor penetración.

eCall

El dispositivo eCall contiene sensores que se activan tras un accidente. El sistema llama al número de emergencias y transmite información sobre el accidente, incluyendo la hora, la situación exacta, la dirección y la identificación del coche.

El dispositivo no estará conectado permanentemente a una red de comunicaciones móvil. Sólo lo hará cuando haya sido activado. Sin embargo, preocupa que esto pueda cambiar, y también la transmisión de otros datos (por ejemplo, para las compañías aseguradoras) y un posible acceso no autorizado a las bases de datos en las que se almacena la información de eCall. Desde septiembre de 2009, todos los coches nuevos de los países participantes irán equipados con eCall.

34. ¿Con qué fin es aceptable la localización de teléfonos móviles? (*Puede marcar más de una respuesta a esta pregunta*)

1. Localización policial de teléfonos móviles de presuntos terroristas y delincuentes con una orden judicial
2. Localización policial de cualquier teléfono móvil sin una orden judicial
3. En caso de emergencia, por ejemplo, un accidente, un niño perdido o una persona desorientada
4. Nunca es aceptable
5. No lo sé

35. ¿Con qué fin es aceptable la localización de coches? (*Puede marcar más de una respuesta a esta pregunta*)

1. Localización policial de coches de presuntos terroristas y delincuentes con una orden judicial
2. Localización policial de cualquier coche sin una orden judicial
3. Localización policial de vehículos robados
4. Control de velocidad e imposición de multas por exceso de velocidad
5. Localización automática y llamada al número de emergencia en caso de accidente
6. Nunca es aceptable
7. No lo sé

36. ¿Debería instalarse automáticamente eCall en todos los coches nuevos?

1. Sí
2. Sí, pero debería ser posible desactivar eCall

3. No, debería ser opcional
4. No, nunca debería instalarse
5. No lo sé

Afirmaciones concretas sobre tecnologías de localización

37. “La posibilidad de localizar todos los teléfonos móviles invade la privacidad”

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

38. “La posibilidad de localizar los teléfonos móviles de un sospechoso es una buena herramienta para que la policía investigue y prevenga el terrorismo y el delito”

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

39. “La posibilidad de localizar todos los automóviles invade la privacidad”

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

40. “La posibilidad de localizar todos los automóviles es una buena herramienta para que la policía investigue y prevenga el terrorismo y el delito”

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo

4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

Retención de datos

Una base de datos se define como una colección organizada de información. Por lo general, se reconoce que cuando pueden recabarse distintos datos sobre alguien, revelan más de esa persona que la información estudiada por separado. Por ello, un principio importante de la privacidad relacionado con las bases de datos que contienen información acerca de las personas es que sólo deberían recabarse los datos necesarios para satisfacer el propósito del sistema, y que deberían borrarse cuando ya no se necesiten.
Últimamente hemos observado una tendencia en la que los gobiernos han pretendido almacenar más información y conectar los sistemas de bases de datos con fines distintos del original, como la seguridad. El tipo de datos a los que más se alude cuando se debate la retención de datos son los relacionados con las tecnologías de la información y las comunicaciones, como los datos del tráfico de teléfonos, móviles e Internet.

Conocimiento Total de Información (CTI)

Conocimiento Total de Información (CTI) era un programa del Organismo de Proyectos de Investigación Avanzada de Defensa de EE UU (DARPA, por sus siglas en inglés). El programa CTI contenía tres categorías de herramientas: traducción de idiomas, búsqueda de datos y reconocimiento de patrones, y herramientas de apoyo avanzadas para colaboración y decisión.
El objetivo del CTI era predecir atentados terroristas antes de que se produjeran. El sistema debía investigar bases de datos privadas y públicas, así como Internet, en busca de transacciones que pudieran estar relacionadas con un atentado. El Congreso de EE UU canceló la financiación del CTI en septiembre de 2003, pero muchos programas del sistema han continuado con nombres diferentes.

Desviación de funciones

Los sistemas de bases de datos son vulnerables a la denominada desviación de funciones, es decir, la utilización de datos con un fin distinto del original. Un ejemplo de esa desviación de funciones se observó cuando la base de datos noruega de buscadores de asilo – que también contiene información biométrica como las huellas dactilares - quedó abierta a la policía para las investigaciones criminales. La intención original de la base de datos era ayudar a determinar la identidad de los buscadores de asilo.

41. ¿Para cuál de los siguientes fines le parece aceptable la retención de información de datos del tráfico de comunicaciones? (*Puede marcar más de una respuesta a esta pregunta*)

1. Para la prevención de atentados terroristas en general
2. Para la investigación de atentados terroristas concretos que se hayan producido
3. Para la prevención del delito en general

4. Para la investigación de delitos concretos que se hayan producido
5. Con fines comerciales
6. Nunca es aceptable
7. No lo sé

42. ¿Para cuál de los siguientes fines considera aceptable la evaluación y la combinación de información personal recabada de distintas bases de datos? (*Puede marcar más de una respuesta a esta pregunta*)

1. Para la prevención de atentados terroristas en general
2. Para la investigación de atentados terroristas concretos que se hayan producido
3. Para la prevención del delito en general
4. Para la investigación de delitos concretos que se hayan producido
5. Con fines comerciales
6. Nunca es aceptable
7. No lo sé

Afirmaciones concretas sobre retención de datos

43. "Las instituciones gubernamentales deberían almacenar todos los datos que consideren precisos por motivos de seguridad durante el tiempo que crean necesario"

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

44. "Los datos de comunicaciones realizadas por teléfono, móvil e Internet no deberían almacenarse, salvo los necesarios para la facturación"

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

45. "La evaluación y la combinación de información procedente de distintas bases de datos que contengan información personal invade la privacidad"

1. Totalmente de acuerdo

2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

46. "El escrutinio y la combinación de información procedente de diferentes bases de datos es una buena herramienta de prevención del terrorismo para la policía"

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

47. "El hecho de que se utilicen bases de datos con fines distintos del original supone un grave problema para la privacidad"

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

Interceptación de las comunicaciones

Pueden utilizarse diferentes aplicaciones para controlar a los ciudadanos y la interacción entre ellos, ya sea por Internet, la red telefónica o áreas definidas. Una forma de interceptación de las comunicaciones a menudo se conoce como *escuchas telefónicas.* Básicamente consiste en instalar un dispositivo de escucha en el recorrido entre dos teléfonos que están participando en una conversación. Se puede pinchar el teléfono del sospechoso o el de las personas con las que se espera que se ponga en contacto.

Una versión ampliada de las escuchas es pinchar de forma más indiscriminada todas las líneas de comunicación (teléfono, móvil e Internet) en busca de conversaciones que puedan resultar de interés.

48. ¿Para cuál de los siguientes fines es aceptable la interceptación de las comunicaciones? (*puede marcar más de una respuesta a esta pregunta*)

1. Para la prevención e investigación de atentados terroristas *con* una orden judicial
2. Para la prevención e investigación de atentados terroristas *sin* una orden judicial
3. Para la prevención e investigación de delitos *con* una orden judicial
4. Para la prevención e investigación de delitos *sin* una orden judicial
5. Con fines comerciales

6. Nunca es aceptable
7. No lo sé

49. ¿Qué método de interceptación de comunicaciones es aceptable?

1. La interceptación policial de todas las líneas de comunicación en busca de una conversación que pueda ser de interés
2. La interceptación policial de líneas de personas con las que se espera que el sospechoso se ponga en contacto
3. La interceptación policial de líneas de sospechosos
4. La interceptación de las comunicaciones es del todo inaceptable
5. No lo sé

Afirmaciones concretas sobre la interceptación de las comunicaciones

50. "La interceptación de las comunicaciones es una buena herramienta para la investigación policial"

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

51. "La interceptación de las comunicaciones es una grave invasión de la privacidad"

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

Tecnologías para reforzar la privacidad

Las tecnologías que contribuyen directamente a preservar la privacidad se conocen como Tecnologías para reforzar la privacidad (TRP).

La *Anonimización* es una de esas TRP. Hay servicios que permiten la comunicación electrónica anónima a usuarios habituales. Esa tecnología oculta la relación entre el usuario y las huellas que deja a su paso y, por tanto, puede impedir la identificación no deseada

La *gestión de la identidad* también es una forma de TRP: en algunos casos, no queremos identificarnos y utilizamos un pseudónimo (por ejemplo, en los foros de

Internet). Para que sea más difícil cotejar datos, puede ser una buena idea el tener diferentes nombres de usuario (que no revelan la identidad) y contraseñas para distintos fines. Los sistemas de gestión de la identidad ayudan a la gente a realizar un seguimiento de sus diferentes nombres de usuario.
La *Codificación* consiste en distorsionar el contenido para hacerlo ilegible a los demás. Debido a que todas las comunicaciones electrónicas son vulnerables a la vigilancia o la manipulación, en muchos casos es crucial que la comunicación se realice en líneas codificadas, o que el contenido que se transmite esté cifrado.

52. ¿Qué tipo de tecnologías para reforzar la privacidad deberían ser de acceso legal para todos los ciudadanos? (*puede marcar más de una respuesta a esta pregunta*)

1. Tarjetas telefónicas anónimas
2. Programas de codificación
3. Gestión de la identidad
4. Ninguna tecnología para reforzar la seguridad debería ser legal ni estar disponible
5. No lo sé

Afirmaciones concretas sobre las tecnologías para reforzar la privacidad

53. "Las tecnologías para reforzar la privacidad son una necesidad en la sociedad actual para salvaguardar la privacidad"

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

54. "Las tecnologías para reforzar la privacidad no deberían ser legales si dificultan la investigación policial y la prevención del terrorismo y el delito"

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Totalmente en desacuerdo

Dilemas en el uso de la tecnología de seguridad

Ahora le plantearemos varios dilemas concretos en el uso de la tecnología de seguridad en proporción con sus consecuencias para la privacidad. Nos gustaría que pensara en las ventajas y desventajas de cada caso y que a continuación respondiera a la pregunta. *Puede dar más de una respuesta a todas las preguntas de esta sección.*

55. El uso de sus huellas dactilares en el metro para registrar cuándo y dónde viaja podría cargar automáticamente el pago a su cuenta. Esto facilitaría mucho el pago, pero implica el registro de sus viajes y el uso de las huellas dactilares para su acreditación. ¿Qué le parecería? (*Puede marcar más de una respuesta a esta pregunta*)

1. Puedo aceptar el registro de mis viajes y utilizar las huellas dactilares en el metro porque facilita el pago
2. Sólo puedo aceptarlo si se almacenan mis huellas únicamente como una plantilla y no pueden reconstruirse
3. Sólo puedo aceptarlo si el registro de mis viajes se borra después del pago
4. El uso de las huellas dactilares debería ser una posibilidad, pero no la única forma de pago
5. Nunca utilizaría mis huellas dactilares como identificación en el metro
6. No lo sé

56. El registro exhaustivo en una base de datos aeroportuaria y la aceptación de ciertas tecnologías de seguridad que pueden considerarse invasoras de la privacidad posibilitarían una facturación rápida en el aeropuerto. ¿Qué tecnologías de seguridad e invasiones de la privacidad aceptaría para una facturación más rápida en el aeropuerto? (*Puede marcar más de una respuesta a esta pregunta*)

1. Aceptaría una verificación y un registro exhaustivos en una base de datos permanente de un aeropuerto y luego utilizar la biometría para la acreditación en las demás ocasiones
2. Aceptaría pasar por la “máquina al desnudo”
3. Aceptaría que se me practicara un escáner para evaluar el sudor, la temperatura corporal y el ritmo cardiaco
4. No renunciaría a la seguridad por un control rápido y cómodo en el aeropuerto
5. No lo sé

57. Las cámaras de vigilancia activas de CCTV y el reconocimiento facial automático en el que se contrasta el rostro de las personas con una base de datos de terroristas conocidos son tecnologías de seguridad que pueden utilizarse para prevenir atentados, por ejemplo, en aeropuertos o estaciones ferroviarias. Estas tecnologías de seguridad posiblemente podrían impedir un atentado terrorista, pero su efecto no está demostrado. También podrían llevar a que se confundiera a personas inocentes con terroristas y a que se las sometiera a un interrogatorio. ¿A qué precio deberían utilizarse estas tecnologías? (*Puede marcar más de una respuesta a esta pregunta*)

1. Las cámaras activas y el reconocimiento facial automático deberían utilizarse independientemente de cuántas personas sean confundidas con terroristas
2. Las cámaras activas y el reconocimiento facial automático deberían utilizarse, pero sólo si existe un índice bajo de personas confundidas con terroristas
3. Las cámaras activas y el reconocimiento facial automático sólo deberían utilizarse si nadie es confundido con un terrorista
4. Las cámaras activas y el reconocimiento facial automático sólo deberían utilizarse en lugares en los que se hayan cometido numerosos delitos o que sean muy vulnerables al terrorismo
5. Las cámaras activas y el reconocimiento facial automático no deberían utilizarse en ningún lugar
6. No lo sé

58. La nueva tecnología posibilita escrutar y combinar información de diferentes bases de datos que contengan información personal con el fin de detectar patrones sospechosos en la comunicación personal y el uso de Internet. El propósito es prever e impedir atentados terroristas, pero significa evaluar datos personales de personas inocentes. ¿Qué acceso policial para buscar y combinar diferentes bases de datos le parece aceptable? (*Puede marcar más de una respuesta a esta pregunta*)

1. La policía debería tener acceso al escrutinio y la combinación de todas las bases de datos en busca de patrones sospechosos que puedan identificar a posibles terroristas
2. La policía sólo debería tener acceso al escrutinio y la combinación de bases de datos si la información es anónima y sólo una orden judicial puede revelar la identidad
3. Nunca debería permitirse a la policía que investigara y combinara bases de datos en busca de patrones sospechosos
4. No lo sé

59. La tecnología eCall podría instalarse en todos los coches nuevos para llamar a un número de emergencia en caso de accidente. La tecnología eCall podría utilizarse también para localizar coches con otros fines, por ejemplo, si son robados o usados para cometer delitos o atentados terroristas, pero esto requiere que el movimiento de los coches que incorporen eCall sea registrado en todo momento. ¿Qué uso de eCall le parece aceptable? (*Puede marcar más de una respuesta a esta pregunta*)

1. Me parece aceptable que eCall pueda ser activado por la policía para localizar un coche si es necesario para impedir un delito o un acto terrorista
2. Me parece aceptable que eCall esté activo en todo momento y pueda ser utilizado para imponer multas por exceso de velocidad
3. Me parece aceptable que los movimientos de mi coche sean registrados en todo momento
4. eCall no debería utilizarse más que para comunicar accidentes
5. La instalación de eCall en los coches debería ser voluntaria
6. No lo sé

60. Las tecnologías para reforzar la privacidad (TRP) pueden contribuir directamente a salvaguardar la privacidad cuando nos comunicamos por teléfono o correo electrónico y cuando utilizamos Internet. Pero las TRP también pueden ser útiles para actividades delictivas y terroristas. Si el fin es salvaguardar la privacidad de la gente corriente, ¿qué riesgos está dispuesto a aceptar para un acceso legal al uso de las TRP? (*Puede marcar más de una respuesta a esta pregunta*)

1. Puedo aceptar las tarjetas telefónicas anónimas, aunque podrían dificultar la investigación policial y la prevención del terrorismo y el delito
2. Puedo aceptar el uso legal de la codificación, aunque podría dificultar la investigación policial y la prevención del terrorismo y el delito
3. Puedo aceptar el anonimato en Internet, aunque ello suponga que las personas que busquen instrucciones para fabricar bombas no puedan ser rastreadas por la policía
4. Puedo aceptar que el anonimato en Internet signifique que las personas que buscan pornografía infantil no puedan ser rastreadas por la policía
5. No puedo aceptar ninguna TRP que pueda dificultar la investigación policial y la prevención del terrorismo y el delito
6. No lo sé

61. Si una tecnología de seguridad ofrece un grado elevado de seguridad, ¿qué consecuencias puede aceptar para las personas que no pueden utilizar la tecnología o se niegan a ello por motivos de seguridad? (*Puede marcar más de una respuesta a esta pregunta*)

1. Puedo aceptar que la gente que se niegue a utilizar la tecnología por motivos de seguridad quede excluida del uso de algunos servicios públicos
2. Puedo aceptar que la gente incapaz de utilizar la tecnología quede excluida del uso de algunos servicios públicos
3. Puedo aceptar que la gente que se niegue a utilizar la tecnología por motivos de seguridad se encuentre con ciertos obstáculos al viajar en transporte público
4. Puedo aceptar que la gente incapaz de utilizar la tecnología se encuentre con ciertos obstáculos al viajar en transporte público
5. No puedo aceptar ninguna consecuencia para la gente que se niegue a utilizar la tecnología por motivos de privacidad
6. No puedo aceptar ninguna consecuencia para la gente incapaz de utilizar la tecnología
7. No lo sé

Cuestiones democráticas

En la próxima sección presentamos algunas afirmaciones sobre cuestiones democráticas relativas a las nuevas tecnologías de seguridad. ¿A quién debería permitirse que ejerciera una influencia en materia de tecnología de seguridad y privacidad y cómo?

¿En qué medida coincide o discrepa con las siguientes opiniones? Indique su opinión acerca de cada punto de vista. Dé sólo una respuesta a cada pregunta.

62. "Los políticos siempre deben someter las cuestiones importantes a debates y sesiones públicos antes de tomar decisiones sobre la aplicación de nuevas tecnologías de seguridad"

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Discrepo

63. “El tema de la seguridad y la privacidad es tan complicado que no tiene sentido inmiscuir a la ciudadanía en debates sobre esta cuestión”

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Discrepo

64. “Las organizaciones de derechos humanos siempre tienen derecho a ser escuchadas cuando se tomen decisiones sobre seguridad y privacidad”

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Discrepo

65. “Es importante que las empresas privadas que producen tecnologías de seguridad tengan derecho a ser escuchadas cuando se tomen decisiones importantes sobre seguridad y privacidad”

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Discrepo

66. “En relación con las decisiones importantes sobre el uso de tecnologías de seguridad, es imprescindible que se ideen soluciones alternativas y se incluyan en el debate”

1. Totalmente de acuerdo
2. Parcialmente de acuerdo
3. Ni coincido ni discrepo
4. Parcialmente en desacuerdo
5. Discrepo

Propuestas para un uso de las tecnologías de seguridad que mejore la privacidad

En la siguiente sección nos gustaría que reflexionara sobre posibles propuestas para la aplicación, el uso y la investigación de tecnologías de seguridad sin invadir la privacidad. Le pedimos que indique la importancia que tendría el llevar a cabo cada una de las propuestas.

Si considera muy importante que se siga la propuesta, marque 1 “De mucha importancia”
Si lo considera importante, pero no una prioridad, marque 2 “De cierta importancia”
Si considera que no es muy importante, marque 3 “De escasa importancia”
Si considera que es de importancia nula o que la propuesta no debería seguirse, marque 4 “Sin ninguna importancia”
Si no está seguro de qué responder, marque 5 “No lo sé”

Propuestas

67. La recopilación de datos personales de individuos no sospechosos debe ser anónima hasta que la identificación sea autorizada mediante orden judicial

1. De mucha importancia
2. De cierta importancia
3. De escasa importancia
4. Sin ninguna importancia
5. No lo sé

68. Sólo el personal autorizado puede tener acceso a los datos personales recabados

1. De mucha importancia
2. De cierta importancia
3. De escasa importancia
4. Sin ninguna importancia
5. No lo sé

69. Antes de su aplicación, debe verificarse el impacto de las nuevas tecnologías de seguridad en la privacidad

1. De mucha importancia
2. De cierta importancia
3. De escasa importancia

4. Sin ninguna importancia
5. No lo sé

70. La financiación de proyectos de investigación sobre nuevas tecnologías de seguridad debería depender de un análisis exhaustivo de su impacto para la privacidad

1. De mucha importancia
2. De cierta importancia
3. De escasa importancia
4. Sin ninguna importancia
5. No lo sé

Preguntas finales

Ha respondido a numerosas preguntas diversas y detalladas sobre tecnologías de seguridad y privacidad. A modo de conclusión, nos gustaría formularle dos últimas preguntas.

71. ¿Mientras cumplimentaba este cuestionario ha cambiado su actitud hacia las tecnologías de seguridad en general?

1. Sí, mi actitud hacia las tecnologías de seguridad en general se ha vuelto más positiva
2. Sí, mi actitud hacia las tecnologías de seguridad en general es de mayor preocupación
3. No, mi actitud no ha cambiado
4. No lo sé

72. Si desea añadir algún comentario sobre las tecnologías de seguridad o algo que no haya podido expresar en este cuestionario, no dude en exponer sus comentarios a continuación: *(cuadro de texto abierto)*

1. No tengo nada que añadir
2. Sus comentarios

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

ANNEX III

TRANSCRIPTS

Group 1

Bueno, como os decía al principio, en la presentación, se trata de que ahora, después de la presentación de la persona experta, realicemos un pequeño debate, donde cada uno exponga libremente todas sus opiniones...
Yo no voy a intervenir, únicamente con alguna pregunta pero ya sabéis que lo que cuenta es vuestra opinión, será una conversación entre vosotros ¿vale?. Entonces, yo lanzo un tema, a partir de ahí empezáis a hablar y ya se va viendo.
Bueno, pues me gustaría que así, ya un poco sedimentando... después de todo esto, si hablamos de tecnología y privacidad ¿qué es lo que primero podríamos decir? ¿Qué es lo que primero que os viene a la cabeza?

Pues que estamos en el sentido, estamos como muy registrados, esta maquinaria lo que hace es que no sea privado nada, es decir, en esta cuestión al futuro pues estamos investigados por todo. La cuestión es que en este tipo de preguntas o debates sobre la sociedad, quiere decirse que vamos a la seguridad en la cual vamos a estar como mucho más investigados, eso es lo que yo creo, y (...) privado creo que no lo somos y de hecho cada vez menos. Entonces ¿es bueno?, ¿es malo?, no lo se. Porque dentro de sí pudiéramos ser privados todos, dentro de (...) pues aquí están los buenos y aquí los malos pues es más seguro, pero por otra parte a nivel de estados y demás pues depende, pude ser muy complicado.

Porque ¿quién vigila al vigilante? Claro.

Claro. Ahí está.

Nos están vigilando, nos están controlando con las cámaras. Y quién tiene todos esos datos ¿quién lo controla?

¿Quién lo controla? Si podemos tener esa seguridad con ellos mismos pues si hay que negociar, el terrorismo...

Pues esos datos, pues si luego hay un cambio de sistema de gobierno o lo que sea, a lo mejor cualquier cosa, los miopes por ejemplo, los socios del atleti están mal vistos por el gobierno que viene pues pumba, están en las listas negras por ser...

Mejor destruirlos ¿no?, no tenerlo siempre

O cualquier cosa

O las cámaras ¿no?, que ponen las cámaras en tu casa o en los parking y algunos quieren y otros no quieren

Luego está la otra forma del que no tiene nada que ocultar, no tiene nada que temer porque si, a mi que me graben, que me vigilen si no he hecho nada malo

Eso es muy relativo porque, en el cambio político antes la huella no existía, yo tengo superior, tengo 54 años y antes estábamos registrados y seguimos estándolo, esos datos no se han perdido.

Pero eso no molestaba

Bueno, hasta cierto punto. Porque de política te podían decir, según los gobiernos, te podían decir que este podía pensar de una manera o de otra, entonces ahí ya te molestaba, ya te llamaban a la puerta

Estábamos vigilados, teníamos que tener una identidad

Es que llegamos a lo mismo no es ser que tenemos libertad, no estamos vigilados.

La cuestión está en como se empleen esos datos

Si es correcto o no

Claro, porque si se emplea de manera efectiva para que todos estemos más seguros, para que haya un mejor control del delito del terrorismo pues yo creo que casi todos estamos de acuerdo en que es bueno, luego lo malo es cuando todo eso se emplea para fines comerciales, que también nos molesta o para fines que a través de Internet pues, por ejemplo, yo creo que hay mucha barbaridad en el uso de los datos privados, e incluso se llegan a meter en nuestras casas a través de los virus que emplean de los space y todo este tema que hay. Y yo creo que en ese aspecto pues lo más importante es el cómo se usen esos datos, si es para bien o para mal.

Y de que forma

Y que la seguridad muchas veces nos la venden, realmente, es el pro de la economía, depende de cómo les interese nos venden la seguridad. Nunca ha estado tan vigilada como desde los atentados del 11-S, entonces desde ese momento todo el mundo tenía que estar seguro, entonces yo creo que ahí ha habido un boom tremendo y nos quieren vender una serie de cosas que... . Y muchas veces se utiliza a nivel económico simplemente porque había uno de los aparatos estos, para controlar los automóviles que decían por ejemplo si te ponen una multa si te excedes en velocidad, pero se niegan a poner un aparto en el que no se exceda más de 140km, pero eso no es en pro de la economía automovilística, no van a vender más coches, entonces ahí ya no. Entonces esa seguridad, sin embargo, no les interesa a nadie. Y nos venden otro tipo de seguridad.

Pues yo pienso que por muchas cámaras, por mucha seguridad que hay, yo parto de la base que los terrositas son buenos, me refiero a que

Que pueden burlarla

No que, a parte de que pueden burlarla, que podrían hacer mucho más de lo que hacen.
Yo imaginaros que yo, que cualquiera pude ser un terrorista, yo me meto en el metro con mi mochila, con una bomba y ¿porque no usan armas atómicas los terroristas? Nunca han usado armas atómicas, que las tienen, de hecho, eso nos dicen que las tienen, las armas de destrucción masiva. ¿Porqué no las usan? Es que yo ya no me fío de nadie ya, no me fío ni del gobierno (...)

(...) entonces puedes llevar el microchip de esos, puede llevarse hasta eso, en el cuerpo un microchip y ya está

Pero yo me refiero a que podrían, yo si fuera terrorista, yo lo veo más fácil entrar en el metro, en el teatro, en el cine, cualquier sitio público, o yo voy al fútbol me meto con mi lata de coca-cola debajo de, y nunca me han pillado, nunca me han hecho nada. Pues igual que llevo una lata de coca-cola puedo llevar una pistola o una metralleta ahí

Sí. Yo creo que nos estamos obsesionando un poco

Por eso te digo

(Hablan a la vez)

Quizá es más libertad para la seguridad de ellos, de los políticos

Exactamente

Es decir, para que los políticos en sí estén más seguros y nosotros estemos dependiendo de ellos, no es otra cosa. Quieren ellos más seguridad

La sociedad de consumo, te meten una cosa que te hacen ver al final que es necesaria, pero en realidad pues no lo se si es tan necesaria

Hombre, yo creo que también es muy necesaria en sitios como los aeropuertos, o en los controles de fronteras que ahí, es un cachondeo, no se si es solo en nuestro país, porque vamos entre los aeropuertos, yo a lo mejor he viajado a, pues mismo a la India y en la India te piden, bueno a mi casi me desnudan en la India y llegas aquí al aeropuerto y ves que pasa cualquiera, pero si pasa hasta un individuo que ha matado a no se cuantas personas en Inglaterra, que ha violado y de repente aquí lo vuelve ha hacer. Pues ahí es donde tienen que utilizar la seguridad, en esos tíos.

Es que en un mundo tan global es que las fronteras son un poco absurdas, porque total que más te da que sea de un país que de otro, no se.

Por aquí decían que nos están metiendo miedo ¿estamos todos de acuerdo? ¿Cómo...?

Hombre pues a nivel de los medios de comunicación están todos los días hablando de si la..., del terrorismo, de todo, yo por lo menos que veo los debates por la mañana es una cosa de impresión vamos

Realmente tienen que hacerlo, porque sino no tienen pretexto para utilizar todo esto y el gran despliegue tecnológico que utilizan.

¿Despliegue tecnológico?

Si no nos metieran miedo ninguno aceptaríamos, si no hubiera un atentado no aceptaríamos que nos escanearan ocho veces para subir a un avión. Está clarísimo que parecería absurdo, si no tuvieras eso en la cabeza, temor de que en ese avión puede haber un terrorista, no pasaría otro escáner al paso de un avión. Yo es que, por ejemplo en un avión si no nos registraron tres veces, no nos registraron ninguna. Y eso, si la gente no tuviera miedo de que puede pasar algo, seguramente no aceptarían hacerlo, es algo que es molesto, es parte de nuestra intimidad porque ven lo que hay en la maleta, lo que llevas, lo que dejas de llevar, lo mismo puedes llevar alguna cosa íntima que no quieres que un policía la vea, pero si tienes que pasar un control pues.

¿Aquí en España te han hecho eso?

Para ir a Egipto.

O sea que, de alguna manera estáis diciendo que se utiliza como pretexto la creación de temores de algo que no existe, es decir, pretexto ¿de quién? Es que esto no lo entiendo muy bien, como...

Tanto como pretextos no, sino como que lo exageran más de lo que es

Lo exageran

Puede haber cierto riesgo, pero a lo mejor no tan alto

Yo creo que no lo exageran para nada sino todo lo contrario, a veces hasta nos ocultan cosas, y al ciudadanos nos tienen, vamos, hay miles de cosas que o tenemos ni la menor idea.

Si porque cuatro periódicos que eliges cada uno te dice una cosa

Cada uno te vende una realidad y cada uno se forma y el ciudadano es el más ignorante que hay, no tenemos ni

Entonces ¿en qué sentido podría ser un pretexto?

En todo caso...

Yo creo que exageran y todo para, por lo menos para que vayamos mentalizándonos.

De todas maneras yo creo que la seguridad está bien.

Bueno, luego a veces nos la creemos de uno, como dices tu cuando vamos a viajar, si no te dicen todos esos requisitos, a lo mejor no te hubieras montado en el avión. Si no tuvieses miedo

¿Si?

Yo creo que no

Pues yo creo que si

Yo por mi parte no porque montar en un avión significa el mismo riesgo que estar en un centro comercial o, es decir, si no se va a poner una bomba en un avión se va a poner en cualquier otro lugar y no puedes vigilar todo eso, es imposible

Por eso te digo que los terroristas, los delincuentes, es que nos perdonan la vida, es que podrían hacer masacres, muchas más masacres de las que hacen. Es que esa es la seguridad que tienen los estados, es imposible controlar todo eso.

Pero por eso es importante controlar la gente que vienen de otros países

Y si vienes dentro del mismo país, y si no estás fichado, simplemente entras en cualquier sitio, enseñas tu DNI.

(Hablan a la vez)

Perdón, solo hay una regla, no hablar todos a la vez
Tú estabas diciendo algo

No pero, yo creo que algunas veces corre el riesgo de confundir porque yo se que me ha pasado que en Miami alguna vez he tenido algún problema y sobre todo después del 11-S y a mi me han parado siempre y me han pedido la documentación y me han pedido que si efectivamente era española y me han parado y me han hecho meterme en las cabinas ¿porqué? Porque podía parecer árabe, o parecer mejicana o puedo parecer, entonces muchas veces te sientes mal en esas situaciones, porque tu no tienes porque, simplemente pro una fisonomía o porque, tu no tienes porque ser una persona que vaya a ser, entonces muchas veces yo creo que ahí llegan a tocar tu privacidad y a no respeto hacia las personas y eso no evita que pueda haber una masacre

Es como la delincuencia, cuando uno ve llegar a un tío con greñas, con malas pintas y tal y enseguida todo el mundo, uy este, y a lo mejor es mucho más

delincuente el que va con la corbata y el maletín, es un ladrón o un asesino y en cambio nadie sospecha de el. Eso es prejuicio social.
Poco a poco la sociedad va cambiando, porque ahora mismo prácticamente la gente joven lleva pintas y nadie mira mal a otro.

Pero yo me refiero a gente que esté fichada en otros sitios, que como entran fácilmente, que luego ves que como este delito lo ha cometido con una persona, pues que ya había delinquido en otro país ¿y cómo ha podido pasar tan fácilmente? Pues hay que, ahí, esos datos pues que la policía los controle mejor, que vaya

Que esté fichado en otros países

..., que es inevitable que no pueden cachear, ni hacer controles a todo el mundo aquí, que vean pues eso, pues ya a un árabe ya tiene que ser terrorista, pues no, o a un, pero bueno, tener un poquillo más de facilidad de datos a través de los países internacionalmente, pues yo creo que es importante.

Pero por eso es parte de las tecnologías

Claro

Yo creo que se ha mencionado, resumiendo un poco, por un lado que hay un despliegue que parece que va más allá de la necesidad que habéis apuntado por razones económicas, por razones de distinta índole que va más allá de la necesidad y en sentido contrario que se queda corto. Entonces ¿cómo compaginamos estas dos cosas? Porque si por un lado decía que se queda corto y cualquiera podría pasar, los terroristas podrían pasar, están pasando las fronteras y por otro lado es desmesurado ¿cómo podríamos...?

Yo creo que a lo mejor opinamos de diferente manera

Yo creo que estamos de a cuerdo más o menos todos, lo que pasa es que (no se entiende)
Si a mi una persona x, ya la tenían fichada de alguna manera o sentenciada, pero por otro lugar había personajillos o gente más baja la cual podría hacer lo que quisiera, entonces si esto se puede hacer, es decir, se va ha hacer las nuevas tecnologías, el meternos un microchip, saber quién somos, pero luego está en quién esos datos o en que casos pueden proceder a evitarnos problemas o nos metamos en distintas políticas o nos metamos en distintos personajes, lo cual es bueno o es malo. Es que no es que estemos todos de a cuerdo, estamos todos de a cuerdo, la toda la sociedad, pero la intimidad de la persona pues no la vamos a tener.

Hombre los avances todo el mundo los queremos

Los ¿perdón?

Los avances de la tecnología, pero luego eso, tiene sus inconvenientes

Los delincuentes siempre tienen la, o sea te ponen un sistema para que no te roben el coche, pero no se ellos antes de que lo inventen ya saben como desactivarlo

Bueno, vamos a pasar un poco, luego iremos entrando en todo esto que habéis dicho. Vamos a pasar ha hablar de los escenarios concretos del documento que os hemos pasado ¿qué opinión tenéis de forma más específica? No hace falta que lo volvamos a leer simplemente ¿Qué es lo que más os ha impresionado? ¿Qué os sugiere?

A mi lo del iris ese, lo del reconocimiento del iris ese me ha dejado, no se si lo vi en una película, en la que ponen el ojo y entonces abren una puerta.

Yo pensaba que no era real

¿Tu pensabas que no era real?

Si.

Al leerlo

Al leerlo

Por lo visto existe.

Pues yo vi un reportaje de unas personas que pertenecían a un club, era un club de alterne, de ir allí a bailar y de tomar copas y se les metía un chip debajo de la piel y con eso pues llegaban y ya consumían todo lo que querían, todo, sin tener que llevar dinero ni nada. Más que, a través de eso, yo creo que eso es el futuro en el sentido de la seguridad, de nuestra identificación, que llegue un policía y que simplemente nos coja la muñeca y pumba

Entonces llegamos a pensar que la chica que nos gusta..., con lo cual estamos de a cuerdo y es un aburrimiento

¿Cómo?

Es un aburrimiento porque somos iguales y nos parecemos y al final llegamos al final.

No, pero eso no es lo que estoy diciendo yo. Que digo que a lo mejor tu nombre, dónde vives, bueno dónde vives no porque ese dato puede cambiar.

Pero ese dato lo tienes.

Es como el número secreto de las tarjetas.

N, pero que no, que el DNI va metido dentro de nosotros.

... te cortan ahí el dedo y te roban todo lo que tienes y encima te han cortado el dedo. Que me roben, pero que no me corten el dedo.

En estos casos que aparecen en los escenarios, ahí el balance entre privacidad y seguridad ¿cómo se daría? ¿Qué se gana y qué se pierde en uno y otro?

Yo creo que tampoco hay gente muy interesada en meterse en la vida de los demás, para fines comerciales si, ver que este tiene este poder adquisitivo o lo que sea, pero no se, no creo que haya nadie interesado en tendencias sexuales, o en consumo, si eres consumidor de hachis o de lo que sea. Puede que haya alguien que esté interesado, pero vamos a quién le importa. Si están interesados algún motivo tendrán
Claro, todo el mundo al final es la economía

Si tu teléfono te llaman para venderte de todo ahora.

(Hablan a la vez)

Telefónica no se como también, es una vergüenza

Eso es muy fácil, como tener una línea, tu apellido y te venden, si te quieren vender una bicicleta

Luego también está el asunto del abuso policial, ahora están saliendo también muchos casos de asuntos internos que han grabado con cámaras, que están metiendo una paliza porque le han cogido borracho, porque vamos no es un delincuente peligroso y hay tres o cuatro policías y que no saben que les están grabando y si han salido de esos casos, cuantos no habrá que

(Hablan a la vez)

La ley del maleante

En ese sentido ahí ¿sería positivo?

En ese sentido yo creo que sí, para evitar abusos, para evitar, pero claro, yo creo que sí.

Y en los robos también.

En los robos

Centros Comerciales que se roba muchísimo

Bueno, pero eso lo tienen

Estamos hablando del escenario este del video control, a través de cámaras

Si, pero luego dicen que no les interesa a las empresas tener demasiadas cámaras, porque al final le cuesta más pagar a los guardias de seguridad, a las cámaras y todo eso que

(Hablan a la vez)

Luego suben los precios que lo pagamos todo el mundo y ya está.

Te asuste más en tu domicilio

¿Y en ese caso?

En ese caso las cámaras de seguridad

¿Y quién te quitaría privacidad?

Depende de donde luego..., volvemos otra vez a lo mismo

Porque ahora por carretera, por ciudad, estás ahora mismo con cámaras y que no vean que te roban la cartera...

Y las cámaras de la carretera son para recaudar, es lo que decías tu que pongan, si no pueden ir a más de 120, pues que no pongan coches que puedan ir a más de 120.

Luego no hay policía, por carretera hay muchas cámaras, pero luego no hay, en los días claves sales y no ves a nadie

Yo creo que también muy importante los estadios y todo eso, que esta gente que se dedica a tirar cosas y no se, de repente tira ahí alguna botella y matar a un futbolista o

O a una persona

O a una persona, precisamente ya lo han hecho, ya lo han intentado

Pero sin embargo le siguen dejando pasar, algún interés tiene que haber en los clubes de fútbol dejar pasar a esa gente

Pero yo creo que eso está controlado porque hay que pasar por puerta y

Ya pero, te gurdas el bote fácilmente

No, pero yo creo que

Yo, vamos he entrado un montón de veces con botes de coca-cola

Yo también. Yo en el bolsillo. A lo mejor te miran la bolsa que llevas el bocadillo y eso

A lo mejor si entras por el fondo sur que están los más peligrosos te registran más.

Bueno, estáis hablando un poco de las fisuras o de la posible ineficacia del control

Sirve el control mas por ellos

¿Por ellos mimos?

Si porque esa paliza que han dado anteriormente a una chica determinada han sido los policías, entonces hay que ver si es por ellos, ineficacia también por parte de ellos, los que están en lo alto pueden hacer y decidir lo que les da la gana. Si les interesa te ponen un microchip, ellos te están identificando de alguna manera y esa persona que te está identificando tiene tus datos, yo tengo el mismo derecho que el que

Es volver al principio de lo que decíais de vigilar al vigilante

Si, justo.

Yo es que creo que todos estos sistemas sirven, mas para, o sea, una vez echo el delito para coger al que lo ha hecho, sabes que ha sido ese porque está grabado que para prevenir. Yo creo que habría que potenciar más la prevención que el delito, que no luego a posteriori.

Los demás ¿cómo lo veis?

Es que yo creo que lo importante sería que estos sistemas fueran realmente eficientes, que no hubiera muchos pero que fueran, quizá menos, pero muy eficientes. Que no hubiera un montón de cámaras y sistemas, sino que las cámaras que hubiera fueran, es decir, el problema de las cámaras es que a veces se equivocan, porque un ordenador no es igual de hábil que una persona viendo caras, entonces dejas una serie de recursos porque, esto es un positivo falso que, lo que tendían que centrarse, en vez, de ser cámaras automáticas hubiera alguien vigilándolas y a lo mejor

Si porque también las puedes engañar

Claro, y

¿Algo más?

Yo, lo que decía antes de que tendría que haber más prevención y menos coger después al delincuente, que es lo que hay ahora.

Es lo que hay ahora

No previenen nada y luego los cogen

Y se van, porque salen por otra puesta

Es que el sistema penal

Bueno. Vamos a intentar hacer un pequeño esfuerzo de síntesis y vamos a tratar de, en este caso lo vamos ha hacer en términos de ronda, vamos a concentrarnos en los aspectos positivos. Vamos a hablar de los aspectos positivos de la tecnología de la seguridad para tratar de llegar a unos planteamientos mínimos en los que estéis todos, más o menos de a cuerdo. Y luego hablamos de lo negativo, para ir un poco cerrando cosas. Empezamos por ti si quieres, el orden lo podéis saltar. Bueno, aspectos positivos.

Aspectos positivos, por ejemplo, que sirva para la seguridad, por ejemplo, te roban un coche y el GPS no, el, puede localizar al coche y al ladrón.

Vale, el GPS para localización del coche ¿qué más?

Y lo de los registros en los aeropuertos también, aunque no sean a veces muy eficaces, pero si

Puedes prevenir.
Más cosas positivas

Pues eso que pueden llegar a la capturación de delincuentes en varios ámbitos, pues eso con las cámaras o encontrando con el GPS del coche. Con esa serie de aspectos pues si que ayuda a la policía a conseguir capturara a esos delincuentes, o sea, en ese aspecto si es bastante positiva la tecnología

¿Más?
Si alguien no ve aspectos positivos tampoco pasa nada

El móvil es positivo. Pero no siempre cambiar el número de teléfono sino siempre el mismo y ese es el que queda constancia siempre.

¿Porqué sería?

Por seguridad.

Por seguridad

Estar con el móvil, digamos tenerlo como carné de identidad. Para todo tipo, tanto de robo, como de seguridad, como de socorro, como de, totalmente, lo llevas siempre. En ese sentido si.

Yo la seguridad, pero yo interpreto la seguridad a nivel general, es decir, por ejemplo lo que tu estabas diciendo. Yo en el documento las preguntas que estabais haciendo o como en los medios de comunicación te dicen una vez y otro y otra, yo es que estoy un poco cansada de la palabra terrorista. Estoy un poco agotada. Entonces creo que es como obsesión terrorismo, obsesión y

venga, venga, entonces muchas veces la seguridad, yo me siento segura cuando, yo que se, si tengo un problema con un policía o tengo un problema con un banco y nadie me protege, o sea, el banco llega y me manda veinte veces una carta y además le da los datos al banco que está ahí al lado y le me mandan propaganda y me llaman por teléfono. O Movistra le da los datos a Vodafone y me llama por teléfono. Eso para mi también es seguridad y sin embargo no la están respetando. Es decir, que yo creo que la seguridad está bien cuando es todo el mundo por igual, cuando hay un respeto hacia la persona o bueno, un control, que me parece bien, también un control que hagan sobre mi. Pero no tiene porque ser, que todo el mundo está cometiendo errores en ese sentido y no se controlan. , A los bancos no se controlan, a las compañías telefónicas no se controla. Se controla a los terroristas, pero no se controla otro tipo de terrorismo que es, el que el banco me está sacando más dinero del que deben

Pero yo creo que es un poco frívolo eso

Bueno, esa es mi opinión, tu puedes tener otra opinión, pero esa es mi opinión. Entonces, para mi es un control que están haciendo y que no me gusta. Entonces me parece bien si se hace a todo el mundo.

Se considera frívolo hasta el punto en que te toque a ti. Cuando te toque a ti la china, o la molestia o

No, pero frívolo en una seguridad en el plan de que no puedan matar a las personas, herirlas o cosas un poco más graves. ¿No? O violarlas, o atentar contra su, o cosas más fuertes.
A lo mejor, los gobiernos y todo eso, quien emplea más las tecnologías de la seguridad para atajar esos problemas un poco más graves. Luego también debería de haber otros controles, a lo mejor a otro nivel, de las personas, de otras personas que controlen a lo mejor los bancos, como dices tu o las operadoras telefónicas de que no nos molesten tanto, ni que nos quiten el dinero, ni todo eso. Pero yo creo que a un nivel un poco más importante lo de la seguridad, pues yo creo que todos estamos de acuerdo en aplicarla en que todos tengamos derecho a que no nos agredan, pues que venga uno y mate a tu hermano o a tu padre o que estés esperando el autobús y te pegue un tiro. O te quiten dinero que te has ganado durante tres meses.

Por eso te digo que por muchos sistemas que haya de estos modernos va a seguir pasando.

Que pase menos

Hombre, pero yo creo que si que ayuda. Seguirá pasando, pero puede ayudar a que se reduzca.

Porque gente mala siempre va haber.

¿Qué más aspectos positivos vemos?

Yo pienso que la tecnología es buena, todo lo que se avance siempre es bueno, pero claro con un control. Bueno yo veo que, así como todo ha sido bueno como el ordenador, el móvil y todo, esto cada vez es, que se yo, para participar en otras cosas

O la vigilancia

Pero yo creo que la vigilancia es hasta cierto punto

Si, ya es mucho

Vigilancia preparada, es que esa gente no está preparada, La vigilancia que está en cualquier sitio de calle, metro o bancos no está preparada.

La clave es eso

(Hablan a la vez)

Es que va más rápido el avance tecnológico que el avance moral de la humanidad, sobre todo del siglo XX para acá

Ahí establecéis un conflicto ¿no? Entre el avance tecnológico y el avance ético.

Gente sin escrúpulos que si tienen a mano usar lo avances tecnológicos los usan para su propio beneficio.

De todos los temores de los que habéis hablado esta tarde, ¿cuál os preocupa más? Vamos ha hacer un poco la dinámica esta de ronda, ahora empezamos al revés. De todo lo que se ha dicho, intentando resumir un poco.

Siempre estamos volviendo otra vez a la seguridad, a la seguridad. Salir a al calle y no preocuparte de tanto de si te va a pasar algo a mi me gustaría ir tranquilamente.
No tener tanto miedo.

Vale, que un aspecto negativo sería el temor este

Un aspecto negativo sería por ejemplo seguridad en mi casa, si tienes seguridad cuando quieren llegar ya se han ido y me han robado, es decir la seguridad que se tiene en las mismas casa en lo relativo a, no es eficaz. Cuando quieren llegar pues ya no están, entonces no es en positivo la seguridad que nos están vendiendo de laguna manera. Seguridad en nuestras casa, seguridad en inmuebles, etc y después las alarmas no funcionan

¿Qué hay poco personal o qué?

(Hablan a la vez)

Seguridad de otra manera, que es más cara, pues vale, que nos pueden vender que la casa no se abre porque tiene otras tecnologías, hasta ahí si. Esa seguridad si que me interesa, Pero esa que pone la alarma y entra por la puerta perfectamente. De hecho cuando vas a hacerte un seguro te dice, bueno, usted tiene rejas, usted tiene

Es como lo que ponen aquí que habían puesto más iluminación en la calle y por lo visto había funcionado mejor que más cámaras. Simplemente que pusieran más iluminación en la calle.
O sea, que a lo mejor hay soluciones que están ahí y no las vemos.

Más simples y más baratas

Más baratas.

Lo que yo oí hace unas semanas que iban a poner cámaras en chueca, no en la montera, en la calle de la montera y en estas zonas que hay prostitución y todo eso y es una ineficacia total ¿para que eso? Si va haber

Vas a ver al marido y va a provocar divorcios y

Si. ¿Qué va a solucionar eso a nivel de...?

(Hablan a la vez)

Esa es una ineficacia total la que pueda tener lo medios de

A mi me dan mucho miedo los errores, es decir, los errores en el que de repente haya confusiones o un error en el que te acusen de una cosa o un determinado delito porque esa cámara dice que eres tu, por ejemplo, y te puedes parecer muchísimo, pero no tienes porque ser tu.

Como el del pasaporte biométrico ese, que una vez que estás lo estás para toda la vida, no puedes cambiarlo.

Ese tipo de cosas, porque yo no se hasta donde la tecnología es tan segura como para identificar, en algunos casos si, pero a mi me da miedo los errores, o por ejemplo cuando escribes por correo electrónico. Yo por ejemplo participo en ONG´s y tal y muchas veces se habla de determinadas cosas que son lo que está ocurriendo en ese país y muchas veces no sabes hasta que punto ya estás vigilada porque creen, no se, muchas veces hay que tener seguridad con las palabras y cosas de ese tipo.

También estoy de acuerdo en ese aspecto, tanto la seguridad tiene errores que molesta a personas que lo sufren. Lo mismo estás en un aeropuerto, como decía el caballero que nos estuvo dando la charla, salta la alarma y ya por eso te meten a registrarte o pierdes el avión y como sea algo de importancia para ti pues ya tienes un problema muy grande y todo por un fallo de tecnología. Porque una cámara, hay una alta probabilidad que una cámara se equivoque, porque hay unas condiciones que ya, simplemente por la luz que te da la

cámara puede confundirse. Entonces ese tipo de cosas pueden ser muy molestas o peligrosas, incluso se pueden crear situaciones de mucha tensión.

La huella en casi todos los países evidentemente si te identifica. Es la más normal, pero luego, es que es tan delicado, es tan complicado, porque a mi me pueden ofrecer dinero, es un ejemplo y entonces para otra persona yo soy normal y llevo, yo que se, bombas.

Bueno, vamos a pasar un poco a otro tema. Se ha mencionado cámaras en las calles, cámaras en los aeropuertos, etc. A la hora de implementar las tecnologías, ¿quiénes creéis que deberían estar involucrados?, ¿A quién habría que escuchar?, ¿Quién tendría que tener opinión acerca de la bondad o maldad o de cuándo o de cómo habría que implementarse estos procedimientos? ¿A quién habría que escuchar?.

En primer lugar los expertos

¿A los expertos?

Tienen que estar preparados.

A las organizaciones de derechos humanos

Organizaciones de derechos humanos

Si, Es lo más importante

¿Es lo más importante?
¿Estáis de acuerdo?

Si

¿Qué mas? ¿Quién más podría estar?

Nadie más.

¿Nadie más?

No hombre si, no pueden ser ellos todo.

Los expertos, las organizaciones de derechos humanos

No se lo que opinará la gente pero, lo que digan las cadenas o lo que haga el gobierno y ya está y que los demás no nos enteremos.

Si lo harán.

Lo que vea la democracia, pues bueno, también porque salga la mayoría, la mayoría no tiene porque estar en el, ¿sabes?, ha salido el PP la mayoría, pues a lo mejor la mayoría está equivocada.

¿Quién me dice a mi que? Es que como desconfío, yo soy un escéptico total, yo desconfío de todo el mundo.
No me creo nada de nadie, y luego me creo todo a lo mejor. Soy escéptico y a la vez iluso, pero no se.

Luego te engañan

Luego me engañas, pero que en un principio digo si, veo la noticia y tal y dices ¿porqué?, o es verdad o es mentira o es media verdad, o es media mentira

Negativo no tienes que ser negativo

Si negativo tampoco soy

Tienes que luchar por algo

Claro, si no entonces no hay nada

Habéis hablado de expertos, de organizaciones de derechos humanos. Tu apuntas, y parece que hay consenso, me corregís si me equivoco, que a las mayorías o a la ciudadanía no porque se pueden equivocar ¿cómo lo veis?

Quizá los políticos no tienen que opinar de eso porque puede ser ya una valoración más personal del político que del bien común. En estos aspectos tiene que ser un poco más, desde un punto de vista de gente experta y organizaciones de derechos humanos conviene más, o conviene más para nuestro beneficio de una forma más objetiva que un político.

En el mismo sentido ¿creéis que debería haber algún tipo de regulación en la implementación de estas tecnologías?

Si.

¿En qué sentido iría esa regulación?

Pues en el mismo

En el mismo que estáis...

Como debería haber una regulación en el tráfico de armas, el la fabricación de armamento, en la hipocresía de los países grandes que venden lo que le sobra a los países que están muertos de hambre y se gastan la mayoría del producto interior bruto en armas, en vez de mejorar la calidad de vida de sus ciudadanos.

(Hablan a la vez)

... su respuesta va en ese sentido a ciudades o países de su seguridad propia

Si, es un proyecto internacional científico, pero aquí el responsable en España es Vincenzo

No claro, le hago la pregunta, si nosotros estamos en este país, que podemos vender armas o las vendemos, es una cosa por la otra. Todo esto y luego por detrás se venden armas porque es todo esto por lo otro.

Pero eso ya no

Ya, pero es el mismo cantar, inseguridad para esto e inseguridad para lo otro.

¿En qué sentido va la pregunta? Dices que esto es una encuesta y entonces que serviría

Quiero decir que me imagino que para la seguridad de los ciudadanos a nivel mundial

Yo creo que trata de comentar una seguridad respetando los derechos civiles

Pero claro, es lo de siempre, es decir, si EEUU está haciendo esto, pero claro luego hace guerras o tiene armamentos, estamos jugando con un doble sentido que ellos mismos están haciendo lo mismo. Las guerras se han ido, han acabado las guerras, pero ahora empieza el terrorismo que les interesa a los políticos ¿esto que es?

Habéis insistido a lo largo de esta reunión en el interés de otros de manejar las tecnologías de seguridad a favor propio, creo que resume un poco el sentido de algunas intervenciones ¿no?, pero ¿quién serían estos otros?

Es la pregunta del millón.

Los poderes fácticos de siempre

¿Los poderes fácticos de siempre?

A nivel económico.

(Hablan a la vez)

Multinacionales

Poder económico.

Multinacionales

(Hablan a la vez)
EEUU está llena de ellos que es los que promueven toda la informática, el futuro...

¿Y porqué están tan preocupados por países como Irak?
Porque hay una riqueza que es el petróleo. ¿Porqué no se preocupan por países como África? Que hay guerra desde hace cuarenta años y...

Yo lo que si que me gustaría aclarar es si realmente todo esto de la seguridad comenzó desde el 11-S en plan, absolutamente con una obsesión, es decir, en plan obsesivo, porque yo creo que antes, se hablaba de la protección de datos que tiene que existir, eso es indudable, tiene que existir y de la protección a lo general, pero yo creo que desde el 11-S ahora es una locura

(Hablan a la vez)

Las teorías estas de la conspiración

Que si estamos

Que al final no fueron los que dicen que fueron, que tal, que no, que fue así

A raíz de ese momento yo creo que ha habido, de verdad ha habido

De ahí la seguridad es para grandes potencias, para países mucho más fuertes, porque a países pobres pues no les dicen nada, pero

Estamos hablando de seguridad de los ciudadanos, no estamos hablando

Pero hay países más ricos que tienen seguridad que otros no tienen y de otra manera se vende a esos otro tipo de cosas

Espera, espera, que esto no lo he entendido, a otros países pobres se le vende

En otro sentido, por ejemplo, yo puedo entender lo que es colombiano, bueno dices esto sucede por eso pero las minorías existen, la cocaína funciona por ahí y entonces la seguridad de que si el mismo gobierno está vendiendo ese tipo de cosas si no tiene otra.
Por ejemplo Venezuela estaba bien y ahora la ha cogido Chávez y a EEUU no le interesa ahora mismo eso, porque puede ser un choque muy fuerte y puede ser otro Cuba, pero viene a lo mismo, seguridad para que si luego esos armamentos, e incluso nosotros estamos vendiendo tanques a Colombia.

Bueno, pero estamos un poco ahí, nos vamos un poco al tema de la seguridad militar.
Me refería más bien a lo que aportan las tecnologías de la seguridad personal de los ciudadanos y en contra de ello, que limitaciones a nuestra privacidad supone, habría que centrarse ahí.
Vamos ha hacer el último balance, vamos muy mal de tiempo.
Me gustaría que hicieses un balance final de ¿en qué situaciones creéis que vale la pena renunciar a parte de la privacidad? ¿En qué situaciones podríais aceptar algo a favor de mayor seguridad?

Muchas

Muchas. ¿Por ejemplo?

La violencia de la mujer, en ese sentido se tendría que tener mucho más esfuerzo, seguridad hacia ese tipo de cosas.

El tipo de delincuentes reiterados, violadores, pedófilos, ese tipo de personajes habría que tenerlos mucho más controlados.

Por ejemplo en Italia que controlen, que no sean anónimos, por ejemplo por una parte claro, todo lo que sea pornografía infantil y tal a mi me parece muy bien, que sepan quienes son los que están ahí.

Es que hay muchas más muertes por maridos maltratadores que por terrorismo, mucho más, yo no se las cifras exactas, pero estoy convencido

¿Qué mas? Violaciones...

Si, delincuencia común.

Delincuencia reiterada ¿algo más?

Si les pusieran un chip a los violadores que salen de la cárcel, que les pongan un chip y que les tengan todo el día controlados, que hacen, como hacen.

(Hablan a la vez)

Claro, si yo robo veinte mil euros y me llevan a la cárcel dos meses y me ponen una multa de trescientos mil, he ganado setecientos mil y vivo toda mi vida de puta madre.

O sea, control económico ¿Qué más?¿Algo más?
Bueno pues ya por último me gustaría saber si la participación en este encuentro que hemos tenido, el que hayáis leído esos documentos que os hemos enviado, la charla de este compañero experto ¿ha cambiado en alguna medida vuestra opinión o percepción o no? ¿os ha aportado algo? ¿habéis cambiado de opinión?

Yo estoy más enfadada.

(Hablan a la vez)

Todos a la vez no, por favor.

Que me impactó el documento, ya sabía ciertas cosas, pero es que me lo leí dos o tres veces porque es que estaba, algunas cosas es que no me lo creía, entonces me enfadé más.

Y tu, perdona que te hemos cortado

Pues eso, cosas que no conocíamos y que me han impresionado.

Te han impresionado ¿en qué sentido?

Pues no sabía que había esta tecnología

¿Qué más?

A mi me ha impactado, desde que vi el reportaje ese de si, no se si es verdad o no, de viajar a la luna, sabía que en ese sentido esto iba a ser así, más tecnología mas

En ese sentido ha modificado tu opinión

No lo que pasa es que me voy a otro planeta, y ya estamos olvidándonos de este planeta, es decir son momentos que van llegando, ahora aquí piensas si vivo en pareja o ese es el futuro sabes

Y lo ves negativo o positivo

En algunas cosas, si es por seguridad lo veo, luego será positivo, pero tu intimidad es que, si conoces a una persona ya la tienes implantada en un aparato y es tu pareja más o menos

Ya, un poco a petición

Si, lo de crear, ya es creativo

¿Qué más? ¿Algo más os ha impresionado os ha llamado la atención?

Si, a mi lo que ha dicho ya, que no pensaba yo que había tantos avances

Hombre todavía no están todos...

Eso del iris y todo

(Hablan a la vez)

... lo del video comunitario, la televisión por cable desde América, ir al médico y que te diga vamos a verte por rayos X, lo van a ver por pantalla, lo pueden hacer desde casa.

Si, eso ya lo hacen en algunos sitios

(Hablan a la vez)

La verdad es que las tecnologías en el campo de la medicina han avanzado muchísimo, no es la seguridad y eso, ahí si que lo veo muy bien también.

Positivo también es para los mayores en ese sentido que están solos en las casas. Positivo porque los están vigilando de alguna manera y no se mueren solos

En ese aspecto si, las chapitas que llevan los mayores es una cosa bastante interesante.

Bueno, pues por mi parte es todo. No se si queréis añadir algo más. Pues gracias.

Group 2

Después de todo esto, de los cuestionarios, de lo que ha hablado Emilio, después de lo que en vuestra casa leísteis ... si mencionamos las palabras, privacidad y tecnología que es lo que os sugiere, lo primero que os viene a la cabeza...

Invasión

Invasión

Yo también, control, mucho control.

Si, a parte del control que es incómodo es necesario, porque es que sino es así pues. Tendremos que amoldarnos a las nuevas tecnologías porque lógicamente todo está avanzando y tenemos que avanzar, entonces pues, es cómo que nos controlan, claro que si, lo que pasa es que bueno dentro de eso la tecnología también.

Está redundando lo que dice la señora es que en épocas pasadas no existían unos fenómenos que ahora han surgido de una manera muy grave como puede ser el terrorismo, como puede ser la delincuencia internacional, entonces es necesario estas y todo el tipo de tecnología que sean novedosas

Hombre es que todas, todas, no se. Yo creo que algunas si pero tampoco, se nota mucho que ha aumentado la seguridad por el terrorismo. Yo no se en otros países, yo aquí no creo que la gente tenga tanto (no se oye), yo personalmente tengo miedo a otras cosas. Si, está bien la tecnología pero que lo apliquen a todo, que no se centren solo en el terrorismo.

Yo creo que está un poco en el terrorismo y está un poco en todo en general, porque por ejemplo las tecnologías también, pues no se, a la hora de moverte, de sacra dinero en un banco de moverte, por ejemplo, el tema de los coches, es fácil que te roben el coche, y por ejemplo me parece muy interesante la tecnología de si el coche tiene un dispositivo especial el cual tu tienes un accidente y puedes estar un poco localizada. Y también cuánta gente se ha

quedado por ahí tirada sin saber dónde estaba. Es como todo, conseguir amoldarse porque hay cosas que nos incordian porque te quitan intimidad y una serie de cosas, pero a la vez son interesantes porque te ayudan dentro de muchos puntos.

De todas maneras eso tendrá un límite de tiempo, de..., porque lo que hayas hecho, lo que hayas podido hacer en un determinado momento no quiere decir que lo arrastres toda tu vida o toda tu familia o todos tus amigos ¿no?. Una cosa que hayas hecho mala en un momento que no vayas arrastrando a todos los que te rodean.

No entiendo ¿qué quieres decir?

Si, alguien puede cometer un delito hoy y dentro de treinta años seguir estando con todos los ojos sobre el y a lo mejor investigando a toda su familia, a todos sus amigos y a toda la gente que tiene alrededor y tampoco me parece justo.

Si, pero, por ejemplo sobre lo que tu dices, la verdad es que desde tiempo inmemorial en España y en otros países existe por ejemplo el RAI, cuando tu no pagas unas determinadas letras y figuras todo el tiempo hasta que no te das de baja en eso. ¿Porqué? Porque es un argumento, a lo mejor para toda la cuestión de banca y demás, para tener la seguridad que no puede dar un préstamo porque son mal pagadores en ese sentido. Entonces, efectivamente no hay más remedio, a pesar de lo que decía la compañera de no tantas, esas medidas modernas para ese tema, pero es que son pocas. Por ejemplo lo estamos viendo en una cosa insignificante, que antes se decía que los países nórdicos eran maravillosos y allí nadie se exaltaba, ahí tenemos el país de este señor que está ahí, el otro día que sale un señor a agredir al árbitro, en Dinamarca, que eso era impensable hace años. Entonces ese tipo de violencia en una cosa como es un estadio de fútbol, eso implica hoy en día que no se salva ya nadie, o sea el “sangre y la” que se decía años a, no existe en el mundo ni somos fenómenos literarios, es imposible ya. Entonces para hacer frente a la cantidad de delincuencia que hay tienen que hacerse este tipo de cosas novedosas, está clarísimo.

Yo creo que más que hacer nuevas o meter nuevas, utilizar bien las que ya hay.

Pero si partiendo de esa base, si partimos de la base de que es bueno, bueno no hay nada, todo es parcialmente bueno o parcialmente malo, o sea no existe el negro ni el blanco, es una cosa intermedia, pero en la cuestión de aeropuertos, en la cuestión de estación de autobuses, de trenes y demás, es que estas medidas son indispensables en este sentido.

Yo creo que ya las que hay... . La típica puerta que pasa los metales... .

Los demás ¿qué pensáis?

Eso, que hay que poner el acento es en los derechos de las personas y de los ciudadanos y que en los estados y en las administraciones públicas deben de

observar detenidamente por esos derechos, para mantener nuestro nivel de privacidad, que por otro lado a lo mejor hay una privacidad a medida de cada uno

Eso ¿qué quiere decir?

Eso querría decir que a lo mejor, cómo podría decirte, yo podría estar de acuerdo en utilizar unos sistemas de vigilancia y otros no, por ejemplo, de alguna manera creo que eso ya lo utilizamos, cuando una persona decide utilizar su tarjeta de crédito en Internet para cualquier compra de unas entradas, pues ya está decidiendo el nivel que desea de privacidad y también de incursión en su intimidad ¿no?. Entonces, a parte de esto, creo que hay que tener unos mínimos que son muy importantes y que la administración debe constituir muy bien para que salvaguarde nuestros derechos como ciudadanos y nuestra privacidad.
Hay sistemas obviamente que tienen que ver con los nuevos, con Internet, con los nuevos medios de comunicación pues que se tendrán que incorporar y depende en que medida se incorpora pues serán más o menos bueno, si esto sirve para que yo tenga un accidente y efectivamente me socorran, pues quién puede decir que no, y quién puede decir que no, que actuando de una determinada manera y mediante un control de datos se pueda detener a unas personas que van a poner una bomba, ¿porqué no?, evidentemente es que nadie puede estar en contra de eso.

¿Qué más?

Es que es eso, es una violación de tu intimidad, pero en cierto modo es por tu seguridad, tampoco puedes quejarte por eso.

Bueno, es lo que yo te estaba comentando, que cada uno podemos delimitar nuestro grado de privacidad. Tu tienes el tuyo y a lo mejor te puedo hacer, te puedo decidir hasta que punto mi privacidad y mis derechos se puede intervenir, un juez o...

Imagino que son tecnologías que se van a programar para la sociedad, no para que tu puedas decir, tu por ejemplo puedes limitar, decir no voy a usar mi tarjeta en Internet porque me la pueden copiar y tal, pero por ejemplo tu vas a un cajero y es que es inevitable ir a un cajero y en un cajero te copian los números, o sea, te copian los números y te están sacando dinero de tu tarjeta, es que no puedes ir por la vida, entonces si no toma unas medidas, entonces no vamos a poder movernos, tampoco tenemos una libertad, nos vana a quitar intimidad, pero también a lo mejor nos dan un poco más de libertad, porque el problema que tenemos es que tu ahora porque no utilizas el, por ejemplo tu tarjeta en Internet porque te da miedo a que te copien ¿no? o porque quieres una privacidad, porque quieres, pero a lo mejor si tuvieses una seguridad porque puedes usarla tranquilamente sin ningún problema, a lo mejor lo usabas. A lo mejor no tendrías ningún problema de privacidad.

Yo creo, que efectivamente, es muy difícil, tienes toda la razón ¿no?, es muy peligroso también.

Es que yo creo que no hay una receta.

¿Qué más?

Que tengas la posibilidad pues de elegir, que introduzcan tecnología, pero que sigan dejando a la gente que no quiere. Hay gente que no le interesa, pues eso, que no te obliguen siempre. El cajero es que es lo que dice, es inevitable, si quiere dinero, casi siempre tienes que ir al cajero

Es que si quieres una seguridad inicial. Si mañana va un señor que es más listo que los señores que han inventado los numeritos y no se que, y que pone una cámara copiando y mañana resulta que vas con la cartilla y resulta que no tienes ni un duro.

Estamos hablando de estas medidas nuevas para la privacidad y sin embargo menos privacidad que hay aquí en España. Toda la cuestión de cuentas corrientes tuyas, en todo momento están fiscalizadas por hacienda, completamente, sin que tu te des cuenta y que nadie ponga el grito en el cielo. Por ejemplo en la cuestión de la declaración de la renta te tienen controlado absolutamente todo, a demás en los propios ministerios te lo dicen, usted ya puede poner cuarenta cuentas corrientes a su nombre que te controlan todo y el señor que no hace la declaración se cree que no lo controlan, pero lo controlan hoy día todo, absolutamente todo.
Antes no tenían esa posibilidad porque no tenía la cuestión de Internet y de ordenadores y tal, pero es que ahora todo absolutamente, cualquier movimiento tuyo diario lo tienen controlado, entonces en todo caso en que intenten, vean alguna operación que ellos crean que no es legal, pero te lo controlan en minutos por no decir en segundos.

Pero todo el tema, tu te alojas en un Hotel o en una pensión, la pensión más cutre que veas y sabe policía sabe que tu estás ahí.

Por eso digo que se ve de lo más natural y no se protesta.

Hombre hay muchas cosas que están, es lo que te digo que todo esto ha salido más por el tema del terrorismo, creo. Es cuando ha sido el boom de poner sistemas de seguridad y claro cuando ponen sistemas de seguridad y cogen datos de la gente es cuando sale... .

No, pero por ejemplo eso en América ya estaba esto bastante bien perfilado incluso antes de lo del 11 de septiembre

Si claro, incluso cuando salió sabían perfectamente los movimientos de los terroristas, antes ya estaban investigando y ya lo sabían, entonces bueno

Para algunas cosas es muy bueno, si vas por ejemplo a un médico y tiene todo tu historial, sabe lo que has tenido, lo que has tomado, lo que no has tomado, entonces eso de que tengan tus datos y el hospital pueda estar en otra parte del mundo ¿no? y sepan de todas tus dolencias, de todas tus... .

De alguna manera una rapidez para cualquier tipo de iniciación de los doctores para tratar a ese paciente.

Y de hecho las tecnologías más avanzadas pienso que está teniendo mucho más éxito, o sea, por ejemplo en Méjico, en Méjico he tenido problemas porque, bueno a parte de la chica esta que la cogieron y tal, pero es que yo, es que mi marido con sus datos nos pasaron dentro, porque allí bueno, la tecnología que tienen es poco menos de hace quinientos años, entonces bueno porque les parecía que el nombre podría, no, si ellos hubiesen tenido otros conocimientos y otras, unas técnicas mucho más avanzadas eso no te pasa. Oye que te meten en una comisaría para estar ahí, pues ya te impone muchísimo. Yo pienso que, lógicamente como para todo, pienso que es para mejorar. Qué nos incordiará, pues simplemente hay muchas cosas que nos incordiará
Hoy decían en las noticias que en los satélites están cogiendo lo que les da la gana, por ejemplo tu estás en tu casa tranquilamente y no se que, te están tomando y luego te lo ponen por Internet. Y parece ser que se puede hacer, que es lo que no puedo entender.

Eso es una de las cosas que nos han enseñado en eso de la cuestión de las nuevas tecnologías que es el de, que a partir de una imagen, se a de una persona o sea de una casa determinada se va avanzando a partir, solamente del inicio, entonces digamos que vivimos el activo más que el pasivo. Porque antes era únicamente el pasivo, se tomaba la cara de la persona o cualquier otro documento y no se profundizaba a través de eso en el ordenador y ahora si se hace, y no solo eso, sino que toda la cuestión de satélites, y en las guerras no digamos, en las guerras están, por ejemplo en Oriente Medio, por ejemplo los israelitas tienen una precisión total, por ejemplo ellos en una casa determinada que ven que hay treinta guerrilleros o treinta terroristas y a partir de una cosa que es completamente, digamos en negro, ya detectan todos los movimientos de esas personas, y por eso después les bombardean pero tranquilamente.

Yo creo que los delincuentes avanzan mucho más rápidos que los que no son delincuentes, me refiero en avances para poder cambiar cosas.

Pero siempre será una minoría con respecto con lo que es, digamos el Estado que tiene muchos más medios para imponer esas normas. Por supuesto que hay muchísimos, aquí en España no tenemos todas las bandas de Cosovares y todas las bandas que han venido del este, pero sin embargo no por eso se va a dejar de intentar profundizar en ese tipo de recursos que antes no existían.

Pero yo lo que digo es que siempre parece que van por delante, eso es lo que quiero decir.

No, pero no creas que ellos ponen, no, la experiencia que cogen, por ejemplo en la sustracción de coches de cilindradas importantes para venderlos después en Marruecos o en la Europa del Este, pero es siempre a partir de las nuevas tecnologías que han implantado.

Bueno ¿qué más?

Son cosas necesarias y nos ayuda a caminar con transparencia, si no tienes nada que ocultar, si dejo el bolso ahí y se me olvida pues, como no hay nada que tenga que ocultar, parece necesario.

No si yo digo que siempre que sea para la seguridad está muy bien, pero es que no solo utiliza, lo de la base de datos y todas esas cosas. Yo estoy harta de que me lleguen cosas por Internet o que abro el correo y tengo sesenta correos todos los días de personas que no quienes son, que no los abro por supuesto. Son personas o son centralitas, pero son correos, porque, de dónde saca la gente mi correo, de dónde saca eso, aunque sea una empresa, me da igual. Si es para seguridad me parece muy bien, yo no tengo nada que esconder, que me miren los e-mail y lo que quieran que puedo escribir cuatro tonterías, pero si es para seguridad, que vean que yo no soy una terrorista, pero porque tanta gente tiene mi correo, es que son tantas cosas. Y te incordian y ya no solo por el correo, por los móviles, yo no se vosotros pero a mi me están llegando un montón de mensajes, un montón de

De números desconocidos ahora

No, de números o de líneas 906 o no se que

Si, para que tu, te `pongas y te cueste un ojo de la cara

Pero tener un poco de intimidad, pero porqué, de dónde han sacado mi teléfono, o sea, es de tarjeta de prepago entonces no se que.

Ya pero eso últimamente y hace muy poco tiempo toda la cuestión esa de, le llama a usted el número tal, pues llame y te cuesta un dinero porque es una especie de 806, claro.

Lo que acaban de decir de la transparencia y de que si no tengo nada que ocultar qué más da, es una afirmación que en otros grupos aparece, ¿qué opináis ...?

Pues yo creo que tiene razón en la mayor parte de lo que ha dicho, si realmente eso es como todo en la vida, si la persona no tiene nada que ocultar puede resultarle molesto el someterse, por ejemplo a ese tipo de controversia en los aeropuertos y demás. Por ejemplo en EEUU hay que quitarse todo, los zapatos y eso fue un boom. Entonces la persona que no tiene que ocultar nada no tiene que tener ningún tipo de problema.

Los demás ¿opináis lo mismo?

Pero se pude invertir.

Se puede invertir ¿cómo?

Si no tengo nada que ocultar, para que tienen que vigilarme.

Es que lo vigilan porque no todos son como tu, por ejemplo, puedes ser una buena persona, pero hay muchos indeseables que van a los aeropuertos y que van además, que intentan pasar cosas, por ejemplo, botes como este, han intentado pasar cosas que aparentemente eran inocuas, y sin embargo eran como se dijo aquí en España el uso del, el que era un detergente y no era tal detergente y eso mezclado con otra cosa podría provocar una especie de explosiones.

Ya pero es que ahora te quitan, o sea, por eso, debido a eso te quitan el bote de colonia que llevas en la maleta, el desodorante, te tienes que ir sin nada.

Pero se ha hecho eso porque es que sino, es que lo han hecho porque no tienen más remedio. Es que no tienen mas remedio. El nivel de delincuencia mundial cuando se mete en EEUU, ha ocurrido casos, que no han ocurrido cosas peores en EEUU porque Dios ha hecho que no, porque sino era imposible.

Para el tema de la droga y esas cosas pero para

No, pero si eso no es de droga, eso es de terrorismo, que eso es aparte.

Bueno, vamos a centrarnos un poco en los escenarios, estos que aparecen descritos en el documento que os hemos enviado y que luego nos ha presentado el experto, lo de la biometría, lo del control por cámaras, base de datos cruzados, etc, todo lo que hemos estado viendo. Vamos a opinar un poco en concreto sobre esos escenarios, ¿qué opinión tenéis? ¿qué impresión os da?

Yo opino que lo de la base da datos cruzados está muy bien pues como lo que han dicho antes, para los médicos, que tu puedes ir a cualquier hospital y ya tienen tu base de datos y tal, pero ya tanto, no hay que llegar a los extremos, lo que ponía en el cuestionario de, por ejemplo, pincharte el teléfono, a cualquier persona. Hombre, si eres terrorista o si en la base de datos de la policía tu estás como que has tenido incidentes o como que te han detenido o algo, pues me parece muy bien, pero si tu no has hecho nada y te pueden

Es que yo no lo entiendo tampoco, que puedan acosar a una persona hasta, no se, porque tenga un fallo en su vida y le tenga que estar acosando continuamente

Aquí en España desde el año 75, cuando empezó el sistema que tenemos ahora, se borraron todos los datos que había en las comisarías, sobre todo a las personas que por lo que fuera, por el punto de vista político, porque habían sido anarquistas, comunistas en esa época se borro todo, eso se borro todo. Eso ya no existe. Lo que está ahora nuevo es a partir del 75.

No solo hemos hablado de bases de datos, hemos hablado por ejemplo de la biometría, vamos a centrarnos ahí.

Eso puede ser interesante. Lo que si que ponía en las hojas estas, en el cuestionario, que es casi imposible de copiar, eso, yo creo que todos hemos visto alguna película, de lo típico, que te hacen una copia de la lentilla con la retina o yo que se, en el caso este que te cortan la mano para utilizar tu huella digital. Yo creo que inventarán algo, algún día van a inventar algo para copiarte, seguro.

¿Qué más?

En el personaje, en los dos personajes que mandasteis vosotros, la señora que se iba a jubilar y el otro que era más bien joven, que era comercial de automóviles, los casos, porque poniendo en boca de primera persona de ella, por ejemplo que se tiene que desplazar de un aeropuerto a otro y que le causaba molestias ese tipo de medidas que se tomaban, y ella reconocía que si fuera por ella no le gustaría que llegara a esos extremos, pero comprendía que para tener mayor seguridad y de todos los que iban con ella, pues

Eso es lo que opinaba ella ¿y vosotros?

Pues nosotros lo mismo.

Yo también, opino que si, lo que hemos dicho antes, si es para agilizar.

Establecéis unos criterios unos criterios comunes a todas las tecnologías de la seguridad, pero podéis establecer alguna diferencia entre las que hemos tratado aquí, es decir, algunas os parecen más invasivas que otras o más...

Por ejemplo las cámaras activas que comentaba a mi me parece mucho más invasivo. Además que eso, lo está controlando una persona, qué criterios está siguiendo para que de repente pues fijarse, no se, puede ser una actitud que tu tengas en un momento dado que para el le choque, pero eso no quiere decir que

Por ejemplo en el caso de este señor que era Alemán creo, el de los automóviles, por ejemplo, cuando se hizo un uso indebido de estas nuevas tecnologías, para intentar relacionarle, pues por lo visto tenía una amistad con aunque era, por el apellido o por el nombre, tenía que ser árabe, entonces le había sometido a un control independientemente de que fuera amigo, entonces le recomendó ella a el que no se le ocurriera mandarle ningún tipo de mensajes, ni de e-mail ni nada, no sea que le relacionara, porque por lo visto un familiar de ella en el país de origen era medio terrorista, entonces claro, sino le involucraban a el, entonces eso si, yo bajo ningún concepto por terceras personas por perjudicar, además lo hacía por una relación de amistad con ella.

Y los demás ¿cómo lo veis?

Yo también, lo mismo, que tengas una persona que conozcas que, no tiene nada que ver con como seas tu, y que, no se, me parece un poco llegar al extremo.

Luego había otra, no me acuerdo como se llamaba, la base de datos que era para el acceso rápido al aeropuerto por ejemplo, y creo que se basaba en que una vez te hacían una investigación, creaban tu ficha y a partir de ahí podrían pasar directamente, o enseñabas la huella o pasabas, pero tu tienes una investigación. Si tu años después entras en una de estas terroristas o eres un delincuente, ¿qué pasa con esa base de datos? ¿y la van actualizando todos los meses?

La vana actualizando

Entonces te van investigando toda la vida

Pero que pasa que te investiguen

No, pero que a mi me da igual pero eso no quiere decir que una investigación inicial, comprueba tus datos, tu tal, tu ambiente, porque bueno, eres una persona de fiar, según pone ahí, como eres una persona de fiar vale, directamente tu pasas y no tienes que pasar control, pero te tienen que seguir investigando para que vean que sigues siendo una persona de fiar.

Ahí, en esa tecnología el planteamiento que haces es que ¿tiene que ser una actualización permanente?, es decir, un seguimiento constante.

No, me pregunto si es así. Creo que si lo hacen, si se llega ha hacer eso, me imagino que lo harán así porque sino no tiene ningún sentido, esa seguridad.

¿Qué ibas a decir?

Si, que eso también es verdad, porque si ponía en el cuestionario que era una primera investigación y era exhaustiva, pero tu puedes tener cualquier incidente o cualquier problema y eso no quedaría reflejado ahí, entonces tienes el acceso tu y puedes crear, como por ejemplo, como el 11-S, otro igual.

¿Cómo? ¿Cómo otro igual?

Hombre es que podrías como otro atentado como el 11 de septiembre. Porque, suponiendo que fuesen aeropuertos, si tienen vía libre y tu ya te has metido, por ejemplo en un grupo terrorista, podrías crear otro.

O sea, que ahí lo que planteáis es una posible ineficacia de esa tecnología.

Si. Bueno, al menos que estuviese constantemente actualizándose.

Que esté actualizado, toda seguridad, ahí en cualquier país y sobre todo en EEUU se actualiza continuamente.

Bueno, vamos a establecer, para que habléis todos y no quede nadie fuera, como somos muchos vamos a intentar hacer una ronda en la que

tratemos de sintetizar los rasgos negativos de estas tecnologías aplicadas a la seguridad, que ya más o menos las habéis mencionado, pero vamos a tratar de sintetizarlos y de llegar a algún planteamiento común o a varias opiniones, no hay porque llegar a un planteamiento común sino surge ¿de acuerdo? Empezamos por ti, por ejemplo, vamos a intentar centrarlo. Lo más negativo

Pues por supuesto el mal uso que puedan hacer de cualquier tipo de base de datos.

El mal uso. El mal uso ¿qué sería?

Pues que no se utilicen esas tecnologías para el fin que supuestamente se pretende, pues para la seguridad de los ciudadanos. Pues mal uso para investigaciones que ya no te afecten a nivel personal o. Que no fuera el uso para el cual se haya establecido.

O sea, que no solo sea para la seguridad

Si

Más cosas negativas

¿De todas en general o alguna en concreto?

Como quieras. Has mencionado antes lo de las videocámaras

Por ejemplo eso me parece que te invade, bastante agresiva, ese tipo de cámaras, de seguridad. Porque aparte creo, lo que yo os contaba, lo que decía creo que llevaba a una persona, una tercera persona, pues eso, que parámetros sigue para decir vamos a seguir a esta persona o esta persona es sospechosa porque, yo que se, ha ido muchas veces al baño y no se que y puede ser porque tengas un problema ¿cómo se mide eso?, qué personas hay detrás como para decir pues si, que parámetros hay que seguir para decir, esta persona es sospechosa ¿quién fija eso? ¿cómo se controlaría eso?

¿Qué mas?

A mi el sistema más negativo que me parece es el de cruces de bases de datos. Porque eso es como una especie de, decir ¿dónde? y ¿quién los cruza?. Puede ser como una especie, yo que se, yo veo ahí a gente que está ahí, efectivamente cruzando los datos de mi vida diaria, del uso de mis cuentas o del acceso a los servicios que hago o del uso del transporte que hago y entonces parece que eso lo hace una gente que no se conoce o no se sabe, y de hecho yo creo que es así, por eso recibimos las llamadas por teléfono que nos venden productos, que podemos o no necesitar o también por Internet nos llega correo, pues eso me parece un sistema más negativo ¿no?
Y en cuanto a, digamos que la sensación que me produce todo esto a lo que soy mas temeroso, es, como he comentado anteriormente, el que se aminoren, que no se respeten no solamente mis derechos sino los derechos de

cualquiera, a estar en mi casa o pasear por la calle sin tener una cámara o persona vigilando

Yo creo que además habría que ver quién va a tener acceso a tus datos, a todas tus datos, a todas tus cosas que son privadas, entonces no se, si son personas de fiar a lo mejor resulta que estás sacando datos a alguien por otro nuevo sistema que lo que va a ser es molestarte o tomarte la vida peor aún.

Eso en otros de los escenarios que hemos manejado ¿dónde lo ves más posible? ¿En las bases de datos cruzadas te están refiriendo o en general?

Yo lo hablo en general, que si son realmente de fiar esas personas que vana tener acceso a toda tu vida vamos.

Si, pues yo igual, más o menos eso, que no se utilicen, que este la nueva tecnología me parece muy bien, pero que se utilice para lo que son, que me sirvan para algo, no para que me bombardeen con mensajes, llamada y tal. Lo que dice ella igual, supongo que eso es una tecnología avanzada y lo utilizarán personas preparadas. No puede tratar cualquier persona, que yo que se, que ahora en muchos casos el circuito de cámaras esta vigilada por vigilantes de seguridad, que es un trabajo como otro cualquiera, pero que no te piden unos requisitos de, no se. Si estas observando a gente y tienes que decidir que esa persona tiene un comportamiento diferente, tiene que tener un mínimo de conocimientos de la actitud de las personas, no se. Bueno, a mi personalmente me da un poco igual que, si es tema de seguridad, si es policía o si es tema así me da igual que sepa dónde estoy, con quién y como, no hay ningún problema, pero si es para tema de seguridad.
Yo de hecho en el metro no me doy cuenta del tema de las cámaras. No me fijo que están ahí, no es una cosa que me obsesione, me da igual, pero que se utilice bien.

¿Y los demás?

Yo pienso, el tema del documento que nos habéis dado, por ejemplo el tema de la biblioteca que a ti te van a juzgar un poco porque si has cogido libros, películas, has cogido una serie de cosas y resulta que a lo mejor, no se este señor iba a por libros para su padre o para una persona mayor de 80 años, entonces que a veces, te digo en la parte negativa, a veces te está juzgando a ti y resulta que tu no vas a coger eso para ti o no eres la persona que va a usar esa cosa y a lo mejor es para un amigo, para no se quién, para tu padre, para un enfermo, para una persona que está mal, entonces todo eso, si hay una base de datos y te está cogiendo que has ido a la biblioteca, que te has llevado cinco libros, este, este, este, este y el otro, entonces...

La interpretación que de ahí salga...

Claro, yo lo veo ahí que es muy difícil, el poderte hacer un seguimiento de tu comportamiento, de tu forma de..., no se hasta que punto eso es interesante, porque de ahí ¿pueden sacar lago?

Si, yo creo que en todas tecnologías sean fiables, es decir no, puedan ser positivos, realmente evitan delitos y no hay ningún problema en admitir que violan tu intimidad. Eso por un lado y por otro yo creo que esos equipos vana acostar un dinero, entonces encarecería en cierto modo los billetes de avión, los billetes de metro, eso habría que pagarlo en algún lado. Y yo creo que encarecería un poco el precio del transporte público, por ejemplo.

Pues yo, el único inconveniente que veo, como ya he dicho antes, son las bases de datos, ya que, según pienso yo o según ponía ahí de lo de cruce de datos, sería de todas las personas. Yo veo bien que sea solo base de datos de la policía, guardia civil, etc, ya que son delincuentes o han tenido problemas graves o lo que sea, pero seguir la vida personal de algunas personas con una base de datos, eso no me parece bien. O que incluso que quede registrado que tu entras a un edificio de Estado, por ejemplo a un Ministerio, pues eso incluso podría pasar, pero que te sigan la vida personal de dónde vas, dónde viajas y tal no lo veo bien.

Yo ya lo he hablado antes

Si

Yo, creo que si es para la seguridad, aunque sea una base de datos cruzada, cualquier sistema me parece bien, y depende también de quién lo haga, si es una persona cualificada o cualquiera.

Cuándo decís cualificada, que ya lo habéis dicho dos veces, ¿a qué os referís? ¿cualificada en que sentido?
La persona cualificada que maneja esos datos ¿es una cualificación técnica o qué?

Técnica, psicológica.

Yo me refiero más que, igual que a esos datos va acceder una persona que es una persona formal, pues se pueden meter los delincuentes y coger cosas que no quieres tu que sepan de tu vida.

Yo pongo lo que decía ella, que como la persona que está detrás de las cámaras como puede juzgar lo que estás haciendo. No quiere decir que vaya a ser un psicólogo, aunque le daría trabajo a todos los psicólogos, no pero hombre, que sea una persona, como dicen en los ejemplos estos, que se andado casos de personas que han vendido las huellas dactilares, por ejemplo. Que investiguen también un poquito, que ya que va a estar dentro de la sociedad, a esas personas yo creo que mucho más porque esta moviendo los datos personal de mucha gente, entonces. Eso, tener un poquito de más control con esas persona s que con el resto.

Si, yo creo que sería sí, como que quién controla a los que nos controlan. Yo antes comentaba eso, que esto debe ser responsabilidad del Estado de

preservar nuestros derechos y debe procurar, efectivamente, que no se produzcan atentados terroristas.

Bueno, en esta dinámica entre privacidad y seguridad, ¿en qué situaciones creéis vosotros o estaríais de acuerdo vosotros en que puede cederse parte de la privacidad en beneficio de la seguridad? ¿en qué casos lo veis?, decís bueno yo sería capaz de renunciar un poquito a la privacidad en beneficio de la seguridad por esto y por esto ¿en qué situaciones?

A mi en el caso del coche, el sistema este del coche, de localización, porque si tengo un accidente me da igual que sepan que estoy aquí o allá, y en algún caso más, no me importa que me fichen en un aeropuerto.

Las personas mayores, a lo mejor si están localizados por algún sistema pues sería muy interesante. Los niños que a lo mejor puedan ser buscados por algo, que a lo mejor tuviesen algún, no se.

Tele asistencia

Tele asistencia a persona mayores.
O sea los coches para posibles incidencias, personas mayores ¿qué más?

Yo creo que fundamentalmente son las medidas que hay para la delincuencia internacional y el terrorismo, eso es fundamental, entonces el ciudadano tiene que saber que ese tipo de medidas que se pongan pude ser perjudiciales a veces, que hay a gente que no le gusta, que le controlen en los aeropuertos y demás, pero es en su propio beneficio. Porque si no existieran terroristas no habría que poner eso.

Bueno entonces en cuestiones de terrorismo, en cuestiones de coche, de...

Yo creo también, es lo que te digo, creo que se centra demasiado en el tema del terrorismo, porque hay mucha delincuencia callejera

Si, pero hay

(Hablan a la vez)

A la vez no por favor

No, el tema este que estaba muy de debate, el tema este de que querían poner cámaras en la calle Montera por ejemplo.

Si, y eso, ¿cómo lo veis?

Hombre, yo he estado trabajando en esa calle en una tienda y la policía desde luego, hay mucha policía o sea que no se si las cámaras iban a hacer algo.

Porque policía ya te digo, yo les veía pasar delante de mi tienda y veía pasar a las prostitutas que se peleaban en la puerta de mi tienda y la policía pasaba al lado y lo veía como algo tan normal, como algo de todos los días que ya no hacían nada, entonces no se si la cámara va a llegar ha hacer algo. Dicen que lo ponen para que la gente se sintiese intimidada y no fuesen a... .

(Hablan a la vez)

En el caso de delincuencia callejera, las medidas de seguridad adoptada, ¿compensaría que se perdiese parte de privacidad o no?

Yo creo que si.

Si

Qué si

En Montera más todavía.

Depende de las calles, claro. Es que son puntos así concretos, que hay problemas, puntos problemáticos, no vas a poner por todas las calles de la ciudad cámaras.

Hemos hablado de los coches, de su localización, del terrorismo, de la delincuencia internacional, del control en determinadas zonas conflictivas de calles, y ¿qué más aplicaciones de la tecnología de la seguridad podría compensar cierta pérdida de privacidad? ¿en algo más?

En el maltrato del hogar.

Eso, cómo sería

Con cámara oculta.

¿Con cámara oculta?

Si, porque con otra cosa.

Pero con cámara oculta en el hogar es muy difícil. Poner una cámara oculta en tu casa, no se, yo creo que eso es muy difícil.

Hombre que te permita, igual que la pones en un bar o en una tienda tienes que avisar a los trabajadores de la tienda.
Entonces la mujer por ejemplo o claro el hombre, depende de la persona que sea maltratada que pueda utilizarlo con su consentimiento, claro.

Pero, no se.

¿Cómo lo veis esto?

Complicado.

Muy difícil.

(hablan a la vez)

A la vez no, por favor

Para ese tipo de productos novedosos que estamos tratando es muy difícil a nivel de hogar, como por ejemplo ocurre ahora con tipo de pulseras o cosas de esas, de agresión en las que le marido la da un maltrato vejatorio, pero lo otro es muy, en un hogar con ese tipo de

Pero lo veríais posible, aunque sea difícil técnicamente.

Si llega un momento que es factible si, no hay ningún problema.

¿Los demás?

Pero ¿quién decide ponerlo? La mujer, el marido, no se

Yo creo que no

Yo creo que en Holanda lo han intentado poner

Bueno, ¿en algún espacio más? ¿en algún ámbito más tendría sentido perder parte de la privacidad en beneficio de la seguridad?

Por ejemplo en la comisarías cuando detienen a alguien, en las guarderías y los lugares donde hay personas mayores y niños que están atendiendo

Y en los grandes almacenes para que no roben tanto

Bueno, ese es su problema.

Y aún así ganan mucho.

Y en conciertos y en sitios así de mucho, bueno de momento tampoco ha pasado nada pero bueno, si que tendría que haber un poco de control. En los sitios deportivos así...

Y de mucha aglomeración

¿lo veis así?

Hombre tampoco, pero es que sino, un poquito más, pues eso, de control, porque muchos casos cuando vas a un partido de fútbol a la mayoría de gente la tienen fichada, pero la dejan pasar igualmente y la lían, y la lían partido tras partido. Entonces pues no se, un poquito más de...

Bueno, ahí ¿qué opináis?

Yo pienso que en los partidos de fútbol, por ejemplo, ahí si que habría que poner vigilancia porque ha habido casos de que han matado a gente y tal, pero

Si, pero se cachean.

Si, claro.

Si y de dónde sacan la botella entonces si se cachea.

Si, se cachea y no te puedes imaginar la cantidad de armas y de navajas y demás que las, y después se las devuelven.

Si, después se las devuelven

O los guantes de béisbol que también los llevan.

Pero aún así los ultra sur siguen tirando,

No, es peor por ejemplo ahí en Barcelona de los Boisos Nois

Y los ingleses

Por aquí decían que es imposible

Si, controlar a todos

¿Y entonces?

En los partidos del fútbol, en el Bernabeu te cachean a todo el mundo.

¿Y dónde dan las botellas?

No te digo que tienen los grandes, para echar la basura y ahí echan de todo lo que no pueden pasar.

Pero no, las que le tiran al árbitro, las que pasan ¿dónde las llevan?

Pero eso es como pasó en Dinamarca el otro día, una cosa imprevisible

Es que no es imprevisible, es que en todos los partidos hay algo, es que se ve que está lleno de cosas que le han tirado a los jugadores. Es que dices, una persona a conseguido colar una botella o un...

(Hablan a la vez)

Y ahí ¿en qué sentido afectaría lo que estamos hablando, la implantación de algún tipo de vigilancia?

No, si aquí está todo, todos los campos importantes en España, cosa que en Italia no hay. Está todo milimétricamente controlado por esa gente, por las cámaras, todo absolutamente. Es muy difícil, en cuanto uno ha tirado algo, porque hay muchos casos que a veces como fue en el campo del Betis o en otro, inmediatamente por esas cámaras le detuvieron y ese señor vivía en Elche, imagínate.

(Hablan a la vez)

Entonces, ¿es eficaz?

Si, si lo es, muchísimo. Es que aquí en España en primera división, aquí son que tienen todas esas medidas.
No, tu no opinas lo mismo. Tu tampoco.

Pero reduce el peligro. El peligro si que lo reduce porque yo puedo entrar con un machete y podría apuñalar a alguien y el machete me lo quitan, aunque luego me lo den a la salida, vale, pero me lo quitan.
Esa es otra, también puedo apuñalar en la puerta, pero yo con un mechero, una moneda o cualquier cosa se la puedo tirar al árbitro.

Pero eso es imposible de...

Claro, luego ya te detienen. O a puñetazo limpio también, es que eso nunca se sabe.

No, pero poner controles, igual que se pone en el aeropuerto de la huella digital o la, que es más fácil yo creo la huella digital, o algún tipo de control también así. Y eso sea una base de datos común pues que en sitios también así pueda utilizar esa base de datos.

Para que luego no puedan entrar.

Claro, para que personas que en un caso puntual, bueno en un caso puntual ha tenido una pelea, bueno, puede ser, pero claro si una persona es que sabes que la va a liar seguro, que no entre directamente.

O sea, que en ese caso también podríamos aceptar cierto grado de mengua de la...

Claro si no le importa que, yo creo, a mi por ejemplo que la policía sepa que yo he ido a ese partido de fútbol o he ido a ese concierto.

¿Algo más en este sentido?
Bueno, vamos a otra cosita. ¿Quién opináis que debería estar involucrado cuando se deciden implantar tecnologías de seguridad? Es decir, ¿a quién habría que prestar atención?, ¿a quién habría que escuchar?, ¿quién tendría que tener una opinión que valdría la pena considerar?

A la población

El ciudadano.
¿Si?

Yo creo que los expertos primero

Expertos

Y por supuesto el gobierno correspondiente

Expertos...

Asociaciones de usuarios

Asociaciones de usuarios

De consumidores

De consumidores

Yo creo que no se puede dejar solo en manos de cuatro expertos y el gobierno, porque está claro que ellos pueden creer que es lo mejor, pero también hay personas del gobierno que han creído que algo era lo mejor y ahora resulta que no, entonces bueno.

Yo creo que tendrían que ser personas cualificadas o bien el ayuntamiento que corresponda o las personas que manden sobre esa ciudad o sobre ese sitio que se va a utilizar eso, porque yo creo que nunca el ciudadano vamos a estar de acuerdo con unas medidas, nunca. Yo creo que a ti te puede parecer bien y a mi mal, a este bien y a mi mal, entonces yo creo que es muy difícil, es muy difícil hablar por ejemplo, el tema, yo que se, no tiene nada que ver, pero el tema de los parquímetros, yo conozco gente que tienen en su calle parquímetros y están encantados y la misma vecina está horroroso y tal, entonces ¿cómo puedes con una opinión de la gente medir eso?, ¿cómo puedes saber si aciertas o no aciertas?. Yo creo que eso sería lo mismo, sería implantarlo y a mi no me gustará y a ti te gustará. Que no es, a lo mejor no es lo más correcto, no lo se, pero a lo mejor si sería lo más...

Lo más práctico.

Es que tampoco se puede, por ejemplo cuando hay personas, de hacer un referente

(Hablan a la vez)

O sea, que por aquí hay un planteamiento que sería dejarle un poco en manos de los gobernantes, que es un poco tu posición, por aquí serían los expertos, tu apuntabas más bien a asociaciones de consumidores y de control de organizaciones de usuarios, eh y a ti te he cortado

Yo también me he ido. No, pero que hay ciertos sistemas de seguridad, pues eso darle la opción al ciudadano decidir si quiere o no ese sistema de seguridad. Entonces dice bueno si, resto un poco mi derecho de privacidad por, a lo mejor, pues eso, para que me encuentren si tengo un accidente o por ir antes, pasar el control de estos, de los aeropuertos, pues a lo mejor eso, algunos sistemas que le den la opción final al ciudadano de decidir o no, no que te lo implanten así ya.

O sea, que ahí estáis un poco en opiniones encontradas porque ella opinaba que...

No, a mi a lo mejor me lo implantan como ella dice y me molestaría, pero a lo mejor, creo que puede ser la mejor cuestión para bueno, me imagino, es como el gobierno, un gobierno hay una serie de cosas que te impone y no te gusta, hay una serie de cosas que te imponen que te parece que son fabulosas, entonces me imagino que no encontramos a unas personas que las cuales tienen que llevar un poco el pueblo, que serán las que tu pienses que lo van ha hacer más o menos..., que luego lo harán mal, yo ahí no me voy a meter, pero bueno que crees que lo van ha hacer más o menos bien. El ciudadano ya te digo, yo creo que esa es una cosa y puede pensar otra o no se, yo pienso que cada uno somos...

¿Cómo lo veis esto?

Es que ese tema es que ha tocado ya tu vida privada, porque es verdad que te pueda gustar o no te pueda gustar en cuanto hagan la ley en el trabajo, pero bueno, te afecta en una parte, pero yo creo que lo más privado que tenemos es nuestra vida privada, o sea, es que si te tocan ya eso y te lo quitan así sin ni siquiera preguntarte, yo creo que ya nada, no te queda nada, que hagan conmigo lo que quieran ¿sabes?. Por lo menos preguntar. No lo van a dejar, evidentemente, en manos ni de las personas, ni de cómo decía asociaciones, pero preguntar, vamos, no se.

En este mismo sentido ¿creéis que sería necesario regular la implementación de tecnologías de seguridad, habría que regularla de alguna manera? O ¿dejarla un poco a que las empresas que desarrollan productos y tal fuesen complementando cosas? ¿cómo lo veis?

Eso lo tendrían que regular

Regular. ¿Y quién lo regularía? ¿cómo veis esto?

Un organismo superior, lo mismo que hay un consejo de estado, como por ejemplo para las leyes que hace el gobierno están de acuerdo al texto constitucional, entonces ese consejo estudiaría esos futuros consejos para ese tipo de iniciativas y dar un dictamen, claro. Que a lo mejor no sería consultivo, sería consultivo, pero no sería decisorio, claro.

¿Cómo lo ves? ¿regular, no regular?

Hombre se ve regular, lo que pasa es que primero se implanta y luego se regula, que es el problema que hay, que vas a regular si no sabes que tienes que regular.

O sea, que viene un poco detrás.

A posteriori, si. Primero tienen bien el sistema y supongo que luego con fallos ya se darán cuenta de que eso hay que regularlo, sino ya invades más cosas de las que se pretendía, o estás vulnerando tus derechos o lo que sea. Entonces es cuando ya, salta la alarma y entonces decide regular eso, porque hay muchas veces que pasa eso.

Y ahí que sería ¿otra vez como antes? O ahí ¿quién regula eso?

Yo creo que las empresas, yo supongo que las empresas pueden hacer las investigaciones oportunas, que ellos piensan necesarias para sacar sistemas de control de la población, que pueden estar más o menos, pueden ser más o menos eficaces ¿no?, pero que si que tiene que estar regulada en la implantación de esos sistemas de seguridad, iba a decir, por el estado que debe velar por nuestros derechos, por nuestra privacidad y también porque no existan delitos, ni atentados terroristas, ni maltratos, ni... Es que es un poco todo lo de antes.

Si, es por centrar temas, no es por... . Estamos todo el rato hablando de lo mismo, claro.
¿En qué medida creéis que os ha afectado...?, ¿se ha modificado en alguna forma vuestra opinión al respecto de las tecnologías de la seguridad, después de este encuentro que hemos tenido?

A mi, en nada.

En nada

No, a mi tampoco. Además se está viendo todos los día y todos los día se están viendo cosas nuevas, entonces, no se, conocer otras cosas, más y tal, peor no me ha cambiado mi manera de pensar.

¿Algo que os haya llamado la atención? ¿Qué os ha sorprendido?

Hombre, no se, yo como le he preguntado antes al señor este que estaba aquí, que en lo de los ejemplos estos, no se, parecía un poco de ciencia ficción en algunas cosas que salían y parece ser que ya existen ¿no?, pero, bueno, pues si, me he enterado de cosas que no sabía.

Si, yo creo que si, que a mi me ha cambiado.

¿A ti te ha cambiado?

Si vamos, respecto a que no soy consciente de todos los sistemas que están alrededor nuestro pendiente de lo que hacemos. Seguramente si dedicáramos

más tiempo pues sacaríamos más cosas todavía. Por un lado si que me ha sorprendido la cosa, si no he entendido mal el sistema ese por el cual, que se ha implantado en Holanda, en un aeropuerto de Holanda en el cual tienes una facturación más rápida, porque bueno, anteriormente has aportado tus datos y tal, pero ese sistema ¿es de pago?

Si

Eso es lo que me sorprende, que sea de pago. Eso es lo que he entendido.

Yo he entendido lo mismo.

Entonces eso es lo que me ha sorprendido, que fuera de pago. Igual que aportas tus datos anteriormente y tal y solo te va a servir para...

Si, pero me imagino que eso lo hacen un poco pues para, tu lo haces para agilizar

No si yo ya se porque lo hacen

No pero es como si vas por una carretera normal o por una de peaje, la de peaje, entonces porqué te metes por la de peaje, porque vas a agilizar, ir más rápido, me imagino que lo que pasa aquí es lo mismo y tienes que pagar.

Si, pero no creo que sea lo mismo. Que llama la atención

¿Alguna cosa más que os haya modificado o no, la forma de opinar sobre este tema?
Bien, una cosa que no hemos tocado, la vamos a tocar un poquito y ya nos vamos, es que entre estas tecnologías, el experto, Emilio lo ha explicado muy bien, hay también el desarrollo de otras, que digamos, contrapesan esta invasión a la privacidad, generando mecanismos de protección de la privacidad ¿no? Esto, ¿qué os parece?

Pues buenas, precisamente para las personas que tienen una cierta propensión a creer que se delimita esa privacidad, el que realmente, si sabe que también dispone de otras medidas para oponerse a la contra liberalización, para por ejemplo, para este señor, estas medidas son impresionantes

Si, ¿son impresionantes? ¿Qué opinais?

Yo es que creo que todo esto es una carrera ¿no? entre la seguridad y

No es que esas son, son totalmente

No, pero deje que termine

Me refería a la carrera desde que el hombre es hombre, para tener una cierta (no se entiende) y para tener desde luego una cierta seguridad de que no se

vea amenazada nuestra existencia y que es una carrera continua, entre crear métodos de defensa, también métodos parta poder vivir, entonces, bueno, supongo que habrá ese funcionamiento y que son necesarios pues otros, es que la tecnología nos aboca a que se diversifiquen todos los sistemas de protección y también de privacidad.

Por ejemplo eso de los mensajes encriptados eso es fundamental para esa cuestión, porque de la duda que el tenía de la invasión de esa privacidad

Eso es un sistema igual que...

Estamos hablando

(Hablan a la vez)

Si, hombre, está bien

Pero esos es para salvaguardar esa privacidad

Es que si vas a encriptar el destinatario puedes encriptar cualquier otro.

Claro.

Bueno, supongo que depende de un código que tengas en común o de un sistema, o de un programa que tiene, es que no se exactamente en que consiste. Yo tampoco lo veo tan impresionante.

¿no?

(Hablan a la vez)

Y a parte de lo de encriptado, también había otra anterior, que tu lo sabrás mejor, que también precisamente se, es que por no sacar el papel que lo tengo aquí, pero si lo veo un momento lo sacaré, era fundamental por la cuestión para los mensajes que se inician, para que no tuvieran acceso a ellos precisamente para preservar tu intimidad.

Veo caras de escepticismo.

Si

Veo mucho escepticismo.

Yo dudo de la eficacia

Tu dudas de la eficacia

Si

Es que se puede hacer cualquier cosa, es que, para otras cosas a lo mejor si, pero el caso de códigos o lo que sea, no lo veo. Yo creo que alguien que quiera decir algo realmente que no quiere que se entere nadie no lo va ha hacer por un medio así, demasiado público.

Eso te pasa con lo del número desconocido que estábamos hablando ¿no?, no se por eso que te pone número desconocido, no se, por lo que sea, por su privacidad, pues prefiere no darlo, claro. Entonces si tienes una llamada perdida no le puedes llamar a el, porque no lo reconoce, pero eso es continuamente los móviles.

Bueno, pues por mi parte es todo, si queréis añadir algo... y sino pues muy bien también.
Pues muchas gracias por todo.

Group 3

Bueno, para empezar yo os propongo que hablemos de lo que os sugiere esto. Cuando decimos tecnología de la seguridad y privacidad... ¿qué es lo primero que os viene a la cabeza?

Esta inquietud, intranquilidad, porque tanto control al final, cuando estamos hablando de cruces de bases de datos, y este control tan frío, me parece que en vez de seguridad lo que tengo es una...

Intranquilidad

Sí.
Entonces, no se, será también que desconozco y me causa mucha inquietud porque yo creo que muchas veces las cosas que surgen por seguridad, a veces hay una serie de poderes que las utilizan mal y se vuelven en contra.

Yo estoy de acuerdo con lo último, es decir, a mi todo me parece muy bien, todos los avances me parecen fantástico, estupendo como se utilicen, si se utilizan para bien fantástico, pero también se pueden utilizar para mal, incluso sin querer. La bobada de poner una cámara y una televisión en Sol y que todo el que se deja caer por ahí le enfocan, ¿y porqué me tienen que enfocar a mí y salir en directo en una televisión? Si yo a lo mejor he dicho que estaba en burgos y dicen, anda mira si está en la Puerta del Sol en Madrid, creo que eso no está bien. Yo no he pedido salir en la televisión. ¿Por qué tienen que hacer un barrido? Mire, y usted que opina. Pues muy mal, a mí quíteme la cámara de encima. No me divierte nada, por ejemplo, puede que no tenga ninguna importancia, pero a lo mejor si tiene importancia porque si yo he dicho voy a Burgos, es que...

Deberían pedirte un permiso

Es que la calle, eso no se debería de hacer

Pero eso no es una cuestión de seguridad. Eso es una cuestión de mala suerte, la tele..., creo

No, de mala utilización de las técnicas.

Es una cuestión vale, de eso, de técnicas, pero no tiene nada que ver con seguridad y en cuanto a lo que estás insegura, es que estoy muy tranquila, me refiero, claro que asusta pensar que hay muchas cosas vigilando y demás, pero yo no tengo la paranoia de que ¿quién se va a dedicar a vigilar a cada uno de nosotros, a cotejar nuestras bases de datos?, no hay un Gran Hermano detrás de todo esto

Parece ser que si por lo que están contando

No, porque sino no pasarían las cosas que pasan, es decir, a mí me parece muy mal momento de hablar de estas cosas con todo lo que está pasando de ETA y demás, y ahora estamos todos como muy emparanoiados con el terrorismo, pero el peligro del día a día va mucho más allá del terrorismo, para mi estas técnicas no sirven, es decir, hacer un escáner a una persona, estudiar su comportamiento, tener su huella digital, me da igual. Tu vecino lo conoces de toda la vida y mañana puede matar a su mujer y más que lo conoces tu no lo va a conocer una máquina.

¿Se previene con estas técnicas?

Yo creo que no se previene, pero tampoco me molesta, es decir, me molesta mucho más que me pille una cámara en la calle si yo le he dicho a fulanito que me ido a Burgos a pasar el fin de semana y me pillan que, que me grabe la cámara del metro.

A la hora que utilizas mi imagen para..., claro tiene una importancia para ellos porque hay público

(Hablan a la vez)

...tenemos Benidorm que bonito, pero hay una señora en tetas o que no quiero que me vea mi suegra de Burgos

(Hablan a la vez)

Todos a la vez no por favor.

Deberían pedir como una promoción de la persona, porque sino te están vulnerando

En el caso del metro que te están grabando, tu sabes que cuando entras ya te van a grabar y sin embargo eso no te garantiza nada, porque tiran a la gente

por las vías, atracan en el metro igual y demás, entonces, a mi molestar no me molesta, pero

A mí en el metro no

Es que pierde su privacidad de coger ya a los que roban y a toda esta gente, al igual que los carteristas y ya que luego que hubiera buenos castigos, que el gobierno o lo que fuera, es que resulta que mucha publicidad, mucho cosa, mucho control para el ciudadano de a pie, pero luego cuando les cogen a estos que burlan todo resulta que además no aplican la ley, no aplican la justicia y no les hacen nada y nada mas que hacen por todos sitios saliendo y yo no se tanta privacidad, si es bueno para coger a quinquis y coger a gente pues...

Bien utilizado sí

...pues acepto, siempre y cuando demuestren los políticos y todos que ellos, pues que. Yo he ido algunas veces a invertir a bolsas, entonces pasa constantemente con un escáner, para allá y para acá, constantemente, y el presidente y todos sus allegados dan la vueltecita entran en el torno este, que entramos a la vez y ellos no pasan por ahí ¿porqué no pasan ellos igual? Y hay que estar pendiente de la máquina esa y salimos, entramos, constantemente y a los demás no, eso ya

Pero bueno, resquicios de esos hay en absolutamente todos los lados.

Pero yo he coincidido con ellos, entran, los dejan pasar y hay un metro de la cámara, pasar también ¿o es que sois diferentes?

Pues por eso para mi las cosas fallan, todos estos sistemas fallan un montón, por ejemplo con la recolección de base de datos, los terroristas otra vez, el que estrello el avión o uno de los que estrellaron el avión, qué ponía en su base de datos, ¿qué había estudiado para ser aviador?,o sea, perdón, piloto. Y que, eso no es peligroso, entonces lo pasan de largo, por eso te estoy diciendo que no creo que lleve a ningún sitio.

Si lo cumplieran a rajatabla todo. Y luego los castigos, todo, todo lo que este.

Vale, pero va mucho más allá de la cuestión de, que estamos hablando ya de leyes, de que se apliquen, de que se queden en la cárcel y todo eso.

La seguridad no es total.

Yo creo que todos estamos dispuestos a modificar un poco, a lo mejor, tu privacidad, yo a lo mejor voy a un aeropuerto y sobre todo, como estamos ahora, que nos están bombardeando y no tenemos mucho miedo y con el miedo también hay muchas cosas que habían conseguido y derechos que tenemos eran pues, entonces tu, tienes parte de ese miedo, Entonces yo voy a viajar en un aeropuerto y a lo mejor digo vale, si eso me da seguridad de que todos estamos pasando y entonces están escaneando, dices bueno, pues a veces te sacrificas para cosas muy concretas, pero no así de una forma

generalizada, sentirte en una sociedad, que te parece eso, pues de ciencia-ficción. Pues a mí, yo por mis años me cuesta mucho y no me gusta.

Las técnicas tienen que avanzar porque lo que van primero, por delante de las técnicas, digamos el hombre bueno, el que no comete atentados ni nada de eso que está realizando ya sea terrorista va por delante nuestra, entonces si se puede convertir en una ciencia-ficción, pero muy deprisa.

Pero es que yo creo, que las grandes bandas organizadas, hay muchas, bueno esos reúnen a todos, a técnicos de, o sea que son expertos, entonces es que eso se está viendo, yo en el trabajo lo veo, o sea, van por delante, entonces eso nos sirve muchas veces al ciudadano de a pie, al que nos está impidiendo, a mi no me gusta que me estén controlando ni el correo electrónico ni, no tengo nada que ocultar pero tampoco me gusta, o sea, a mi me gusta observar mi

Yo opino que todo lo que sea mejorar la seguridad no me molesta, pero siempre que no se vuelva en contra.

Claro

¿Qué es ponerse en contra?

Me refiero que me gusta tener mi privacidad. Lo que ella decía, salir un momento determinado, que te cojan ahí en una pantalla de televisión, que tu hayas dicho que vas a otro sitio, así por decir algo, eso es lo que me molesta, pero por lo demás como que estoy tranquila. Y que no siempre del todo, hombre, me imagino que la seguridad irá mejorando también.

Ya, pero también háblanos de datos

Las nuevas tecnologías irán quitando poco a poco riesgos para que tampoco pierdas, casos más concretos, el que se use de una manera.

No te entiendo bien, o sea, que la seguridad va a ir avanzando...

Me refiero que las nuevas tecnologías y eso, que yo me siento más segura de las nuevas tecnologías para la comunidad, pero también me molesta un poco perder la privacidad, eso a nadie nos gusta, pero claro, para tener más seguridad, también tienes que perder un poco de

Siempre que sea necesario, cuando te hablan aquí con una orden judicial, cuando yo sepa, yo puedo ir a un sitio y aceptar una cámara porque yo se que existe esa cámara, yo elijo y también que me den la seguridad en algún momento, entonces por lo menos, que yo sepa. Y que siempre, o sea ya, haya un control, que, no se, que un gobierno tampoco puede aceptar, que no es todo válido para la seguridad, y en estos ejemplos que se vena aquí, en estas opciones, es muy evidente, o sea, con un, hay dos personas que emprenden un viaje y aquí van en paralelo, entonces a mi me parece que la actitud de la señora esta es mucho más reflexiva, o sea, que a mi me parece que es un uso, que ya tiene un opción, o sea, ella elige una forma más responsable, más

represiva. Al otro le da igual, pero al final se encuentra que ya no, que no tiene nada, él dice que ya no, él tiene una discusión con un amigo, que el amigo es un obseso de la privacidad y él es todo lo contrario y dice si yo no tengo nada que ocultar, pero al final ya, cuando quiere llamar a su amiga esa o cuando ya hay algo que le incomoda porque ya es demasiado, entonces se encuentra envuelto en esa espiral y ya ni siquiera controla. Yo desde luego no estoy, yo opto por la actitud de la señora esta.

Carla

No por la del chico este, por la del otro, que todo vale, todo vale, todo vale, pero al final pues.
Yo me parece muy bien todo ese sistema para ayudar, para prevención, de una forma razonable, y sobre todo, muchos sistemas de esos pueden tener un uso, todas las tecnologías bien aplicadas pueden tener un buen uso. Entonces, para lo de los accidentes, que un coche tenga ese sistema, para localizarle si tiene un accidente, pues me parece perfecto, igual que el móvil, también en los infartos y todo eso se ve que mucha gente se ha salvado, pero el uso

Yo, personalmente cuando he llegado aquí, yo decía que estaba muy bien lo de las tecnologías de la seguridad y eso, pero me ha desconcertado mucho el cuestionario que nos han puesto. Yo creo que realmente las tecnologías de seguridad que nos está proponiendo, van a ir más a nivel de comercios, de que no haya seguridad de policía, sino a nivel de instituciones privadas, que no tiene nada que ver con la seguridad personal, sino más bien con, estamos haciendo lo de la biometría para ver que datos podemos obtener y que podemos venderte, no lo veo como seguridad, sino como más bien como inseguridad. Porque yo al principio decía, bien para la seguridad, pero yo creo que eso se enfoca para, el estado público no lo va a subvencionar, más bien son lo que son las empresas privadas. Entonces, va ir destinado también a eso y yo pienso que a mi me parece horrible, por ejemplo que en un comercio se vaya a poner lo de la biometría y que te digan, como dijeron, ¿qué tal la compra de tu raqueta o no se qué? Que sea para venderte, porque si es para evitara terroristas y todo eso, pues yo lo acepto, pero yo creo que todo esto es para venderte y no para la seguridad, ya para

Un estudio de mercado

(Hablan a la vez)

Eso se está haciendo totalmente, se llama CRM, gestión de clientes y softwear ¿no?, que analizan todas las compras de tus tarjetas, interrelacionan consumo, te hacen ofertas específicas según tu gusto, si se hace bien, pero muchas veces se, como este, invade un poco ¿no?. Desde la llamada telefónica que alguno a veces quiere dormir la siesta y tiene que desconectar el teléfono porque sino, me vana llamar a las cuatro de la tarde para ofrecerme, eso también es una invasión a la privacidad, yo lo tendría que autorizar eso.

Si, una publicidad que tu no tienes que ver con esa empresa, no la has visto en tu vida y te lo mandan con tu nombre, dirección, apellidos...

Lo sacan de una base de datos y tu cuando te apuntas a cualquier, me refiero, cuando cualquier persona se apunta a un sorteo o rellena una tarjeta para pedir una tarjeta o lo que sea, tiene por ahí

Una tarjeta ¿de crédito te refieres?

Una tarjeta de Alcampo, tu tienes tu cuadradito en la que acepto que mis datos vayan a una base de datos, si o no, en el momento en que tu das el si, te arriesgas a que

(Hablan a la vez)

A mí nunca me han hecho esa pregunta y yo si sale digo que no. Pero yo el otro día, que es lo que iba a contar antes de que, pero no tenía tiempo ni ganas de discutir con una niña encantadora que estaba en una tienda de Movistar, yo iba a cambiar de móvil, entonces me pidió un número de contrato, sencillamente porque mi teléfono es de contrato y le dije, no me acuerdo igual otra cuenta, y me dijo no te preocupes si no te importa me meto yo en... y le di mis datos y se metió en el ordenador y sacó mis datos de la cuenta, yo le di mis datos y ella sacó mi número de cuenta

Pero con el número de teléfono tiene todos los datos

Pero eso es demasiado

Es demasiado, es demasiado

Y ¿has hablado otra vez con Movistar?

No, no si yo iba a cambiar otra vez el teléfono. Y el que si fijo, que si tarjeta, que toma que dale, y yo tenía prisa y ella ¿eres fijo? si, y dice dame tus datos y dice, el número de cuenta y digo no el número de cuenta no lo se, digo bueno vivo aquí al lado. ¿Ella porque tiene que tener?

Porque lo has dado una vez y

Una cosa, ¿podríamos establecer diferencias?, hemos visto aquí en la entrada que habéis hecho, vuestra opinión general sobre este tipo de tecnologías, bueno, no voy a resumir porque creo que ha quedado muy claro cuales son vuestros planteamientos, pero ¿podría establecerse diferencias respecto a las distintos tipos tecnologías o de técnicas aplicadas a la seguridad que nos han comentado, que hemos visto en los escenarios del estudio?, es decir, por repasar un poco, hemos estado viendo las mediciones biométricas, el control por cámara, el cruce de datos, el control de los flujos de comunicaciones, los localizadores, en fin, las tecnologías aplicadas a la defensa de la privacidad. Todo esto que nos ha explicado antes Emilio, ¿podéis establecer diferencias o lo veis todo igual? ¿podemos establecer diferencias o es todo lo mismo?

No, hombre yo veo bien el eCall ese que es para, pero solo cuando tengas un accidente que se active, pero yo por ejemplo para que me encuentren o localicen pues para eso si quiero con un GPS ¿no?, y por eso si lo veo bien, pero hay cosas, como la máquina al desnudo que eso ya me parece una aversión vamos

Horroroso

Cosas que son, que van más allá de una cosa normal, no se. Por ejemplo, una máquina para detectar metales y eso o que haya perros policiales por si llevas drogas y eso yo lo veo lógico, para que no haya contrabando, terrorismo, pero ya una máquina al desnudo y cosas así, que ya como que no tienes ni privacidad ni nada, es como, solo me falta decir lo que pienso para que me conozcan entera no tienen, no

Y rayos x, rayos x porque gente que lleva droga en el estómago o en el intestino o dónde sea o esos como se llamen, tienen rayos x, las bolitas, las pelotitas

Eso es lo que ha dicho de una alternativa, porque nosotros debemos de plantearnos lo que el estado nos quita que lo que nos queda a nosotros

Pero por ejemplo, lo de los perros llama más la atención porque estás menos acostumbrada, pero puede llegar a ser igual de denigrante, o sea, yo tengo a una conocida, muy conocida que, rápidamente, ha estado en EEUU y un perro le debió oler algo en el bolso, le arrancaron el bolso de la mano, le tiraron el bolso al suelo, el perro lo mordisqueo, tal, no tenía nada y el agente ni se agachó a devolverle el bolso, ahí se quedó tirado. Me puede parecer igual de humillante que me vean dos pero0snas, que se que están velando por mi seguridad, que te vean las formas a través de una pantalla o lo que sea. Si dentro de diez años todo el mundo tiene que hacer eso cuando pasas por un aeropuerto te parecerá más normal, creo yo.

No, por ejemplo si tu, yo ahora mismo estoy en una etapa, a lo mejor, que me da vergüenza mi cuerpo ¿no?, que todavía no lo he llegado a aceptar y que una persona que no le he dado permiso que me vea, pues me parece

Pues, yo tampoco, tampoco me mola delante de nadie, pero lo que me refiero es que, depende de lo que te estés jugando, depende de lo que tengas dentro de la balanza, hoy por hoy si te quieren desnudar te desnudan, si te quieren intimidar, te pueden intimidar

Pero eso hay varios grados, según las técnicas estas existe el escáner ese del desnudo, luego en el maniquí y luego lo de detención, o sea, lo de los metales, es que no es lo mismo una cosa que otra

Pues por eso, como no es lo mismo una cosa que otra, vamos a ver si tratamos de establecer diferencias, no se si llegamos algún tipo de acuerdo sobre una posible jerarquía entre las distintas tecnologías de las

que estamos hablando esta tarde, en términos de cesión de privacidad, beneficio

Para nosotros son unas tecnologías muy nuevas, que aunque lo leas aquí, no sabes ni lo seguras, ni cuando dicen, ahora mismo, te roban los datos, es que primero tengo que saber, tengo que contestar yo como, tengo que saber como se hace eso para saber si no es seguro. Entonces, el iris, pues cuando estoy, según el libro este parece que el iris no es tan agresivo, es más, es que lo desconozco, entonces tampoco puedo opinar, pero entre leerme el iris o grabarme la cara, pues casi prefiero que me lean el iris.

Vale, los demás.

Yo tengo que ver si es malo para la vista

Claro, si

Yo pondría primero el eCall del coche

Ese parece que... . ¿Coincidís todos?

Si

Si, si se activara en el momento del accidente, sí. El que te puedan rastrear en todo momento eso ya sería más invasivo.

O sea aquí hay una condición, que sea voluntario., dos que se pueda rastrear, que no sea invasivo en todo momento, sino cuando hay una deliberada conexión digamos.
¿tu no? Pues vamos a ver, esa es una opinión, vamos a ver otra.

Yo creo que, que por ejemplo, lo que os comentaba antes, yo no creo que tenga a un Gran hermano vigilándome en cada momento, a mi por ejemplo, dentro de que yo no hago esas cosas, a mi lo que no me interesa es que mi marido me pille una mentira, por ejemplo, no que un satélite GPS me esté mirando. Entonces, si yo tengo un accidente, a mi me gusta que haya un satélite que me pueda localizar. Si mi marido no sabe lo que yo estoy haciendo, tenga yo el GPS, tenga el eCall, no va a ir a buscarme a la vez, es decir, que esté localizada con GPS no significa que

Pero si tu lo has instalado lo estás decidiendo tu

Claro, yo lo decido evidentemente, pero que yo soy partidaria en cualquier momento, en este caso concreto, por ejemplo en lo del coche, incluso en el móvil. A mi no me importaría llevar un chip en el móvil que si en un momento dado, la policía, yo que se cualquier cosa, me tienen que localizar por una emergencia que porque yo lleve el móvil me pueda salvar la vida, a mi me da igual

Si a mi, a lo mejor, personalmente no me importa, lo que pasa que yo no estoy pensando solamente en mi, estoy pensando en todos y en los...

Bueno, vamos a ver. A ver si os parece que llegamos a un mínimo acuerdo que es lo más aceptable, con las condiciones que habéis puesto, que sea opcional, tu dices lo de tu marido...

Si, yo lo pongo, pero esa información no la va a manejar mi marido

Vale. ¿Estáis de acuerdo en ese planteamiento?

No

No, tu no, a ver.

Yo creo que si quieres que te localicen por eso llevas un GPS o te llevas el móvil o lo que sea, pero, si tu no quieres ser localizado porque no te da la gana, pues yo no creo, ni la policía ni nadie, que te tengan que encontrar, a no ser que seas un terrorista o algo así, que tengas antecedentes o lo que sea, entonces si es lógico que te quieran detectar, pero sino no eres una persona, a mi ¿para qué necesitan saber dónde estás?, porque ni tu marido ni nadie si no quieres.

Tu en ningún caso. Bueno, esa sería la más, la menos invasiva la veis quizá...

También porque es la más opcional

La que es más opcional

Claro porque la puedes activar en cualquier momento

En caso de accidente sirve como identificación, es igual como meterse un microchip y si quieren pueden ver en todo momento donde estás, es lo mismo. En tu auto, en cualquier momento, yo no sabría tampoco, sentirse perseguido, pero para qué utilización o que se podría

Asegurar que va a ser seguro para...

Porque a lo mejor los fabricantes de tal modelo quieren saber por dónde andan sus usuarios, eso a mi no me interesa que lo sepan, qué estudio, porque se va a utilizar para fines comerciales, estoy segurísimo, como base de datos y toda la información que puedan recabar.

En eso insistís mucho, en la utilización comercial de la información. Insisto yo un poco en la pregunta que os hago ¿igual para todos los casos? O veis algunas de estas tecnología más proclives a ser mal utilizadas.

¿El caos comercial?

Si, es que es en lo que estáis insistiendo.

Yo en comercial en los datos.

En el cruce de datos

Si.

Y la biometría

Para hábitos y cosas de esas.

No se, yo he leído hace poco en la prensa que como que en los Grandes Almacenes hay una serie de, no se, rayos infrarrojos o algo así, que detectan tus movimientos para saber donde pasas más tiempo, donde..., a mi eso no me parece bien.

Eso lo tienen como...

Es marketing, que depende la música en cada, con qué música se vende más, es que se ha llegado hasta ese extremo, es decir, depende de una música la gente se anima más a comprar, no se, alo mejor si ponen sevillanas dices ¡ele¡ me voy a comprar unas castañuelas...
(Risas)

¿Podemos establecer más diferencias para temas comerciales? que es, digamos la utilización perversa que le veis al asunto, con la que más, riesgo se corre sería las bases cruzadas...

El pinchazo telefónico

Esa, ¿en que sentido?

Porque si quieren, te pueden escuchar toda tu conversación. Si no eres sospechoso de nada, no tienes una orden judicial, ¿para qué quieren saber lo que estás hablando con una amiga?, y puedes estar hablando de tu vecina

Eso es lo que me llama la atención a veces, si quieren te escuchan.

(Hablan la vez)

Todo esto yo creo que cuesta mucho dinero y nadie va a tirar mucho dinero para nada, para oír lo que le estoy contando a mi vecina. Está claro el caso comercial, que yo no lo veo como vosotros, el comercio que te quiere sacar pasta y que te quiere vender algo te lo vende con solo mirarte, sin que te lo propongas, me refiero...

Pero hay comercios que...

Pero puede haber una conversación que sea de negocios o algo así que a alguien le interese escuchar, y a mi, no es mi caso, y alguien si que puede estar interesado, o cosas, o los políticos, o

Pero eso es una cosa ilegal

Una pregunta que se ha hecho, parece interesante, hay una referencia constante a alguien, es decir, ¿quién podría estar interesado a un mal uso de esto?, antes habéis mencionado empresas privadas que pudieran estar detrás, ¿quién creéis que podría utilizarlas mal? ¿quién sería ese alguien que hace un uso provechoso

Pues la competencia

Delincuentes

No y la competencia

Delincuentes que están compinchados con gente que controla esos sistemas, eso es el pan nuestro de cada día, eso se ve, las bases de datos, hay muchísima venta de datos a delincuentes, porque (no se entiende) y se consiguen, entonces los primeros para cuando se está vulnerando ese control, pues muchas veces es esta gente, porque el dinero, es que funciona, que da dinero, tal, la gente se sorprende. Entonces, los delincuentes porque le interesan y luego también en, yo creo siempre, el primer factor es el dinero, el dinero, entonces, negocios, política, cosas de esas de poder

¿Y los demás?

Bandas organizadas

Yo es que vivo muy tranquila de verdad, me refiero, que claro que por supuesto que todos tenemos un factor de riesgo, pero yo no creo que nadie, o sea, si me quieren timar, sacarme el dinero por Internet, por ejemplo, evidentemente esto es una ayuda, eso de que tengan base de datos y demás puede ser una ayuda, pero pueden pasar tantas miles cosas sin esto de por medio que no tengo el temor de que nadie esté vigilando lo que hago

¿Qué más? ¿Quién creéis que puede estar?

Las empresas privadas, quién maneja el dinero evidentemente, yo pienso que pueden estar interesadas en la biometría para conocer los hábitos de consumo y todas esas historias porque como dice ella, el dinero mueve el mundo y

Yo creo que una cosa, que a veces se consiguen más las cosas porque interesa más a la gente que pierde o gana mucho dinero que por tu seguridad, que estoy segura que ahora mismo que se están, con todas estas nuevas tecnologías se están aplicando y ¿quién van a ponerlas en funcionamiento?, los bancos con las tarjetas de crédito, porque es que les interesa, las aseguradoras, ¿y quién también en estas cosas va a tener...? o sea, cuando

estamos hablando de la biométrica, si a mi me detectan, si yo tengo que pasar por un escáner y a mi me van a controlar si yo estoy enferma, si..., siempre tenemos miedo, yo no tengo miedo, es decir, que no son miedos personales. Yo no soy miedosa a parte de que diga todo eso, o sea, personalmente no me considero una persona con mucho, además pongo, soy, pero si me inquieta que cosas que han costado mucho, o sea nosotros tenemos, estos puntos que hay aquí que a mi me parecen importantes sobre la declaración de derechos humanos de la privacidad, a mi me da, esto si me inquieta que, que poco a poco, esto que está aquí reflejado en el "los expertos temen que esto desemboque en una pérdida de la privacidad para la sociedad, que sea difícil recuperar una vez desaparecida", nos estamos acostumbrando, nos parece que todo es válido y no me parece que esté bien, o sea, que todo sea válido. Yo creo que hay cosas que son necesarias y lo que es necesario pues vamos a aplicarlo para ese fin...

Vamos a ver si hablamos todos. Los demás ¿estáis de acuerdo con ella con ese otro planteamiento?

Yo estoy totalmente de acuerdo

Creéis, como dice el papel que acaba de citar y que habéis recibido vosotros, que nos vamos a acostumbrar a una pérdida de privacidad poco a poco y que vamos a perder las conquistas realizadas en relación con los derechos civiles y con los derechos humanos ¿creéis que estamos en esa situación?

Yo creo que ya está pasando, por ejemplo el softwear que trabajan a nivel de satélites de comunicación donde analizan palabras o frases o interconectadas y demás que están analizando. Yo no me siento perseguido por eso, pero me parece que es, uno se está habituando a ese tipo de cosas, como que te lo tomas como normal, me parece como problemático.

Yo pienso que es como te tomes la seguridad, si es prevenir o castigar

A ver, di

Si, porque según en que sitio estemos o en que época estemos puede ser más aceptable el tomar ciertas medidas al que nos parezca un poco, violar nuestra seguridad, que a la hora en concreto de, por ejemplo a la hora de saber a lo mejor que están escuchando personas concretas (no se entiende)
(risas)
no se, pro ejemplo con el 11-S, todo lo que hubo pues se radicalizó mucho y la gente lo veía normal y ya no solo eso, sino que ya es prevenir o controlar a todo el mundo y yo lo que veo que la seguridad según como se plantea está para prevenir algo, las prevenciones son a modo social de ver a la gente, porque todo eso no viene siempre pensado en el terrorista, el terrorista es una persona que tiene su vida, tiene sus cosas y el reconocerle facialmente bueno, podemos detenerle y vendrá otro y vendrá otro, y porqué viene tanta gente

(Hablan a la vez)

Demasiada policía

Claro, un estado nazi que parece que para ellos a lo mejor era válido, porque claro, intentamos detectar con las S.S. los que están en contra del sistema, para ellos era válido. Uno se va adecuando, a lo mejor, a un sistema totalitario también que, por los terroristas o por

Pero ese depende también de la época

Claro, lógico

A lo mejor lo vemos ahora un poquito de ciencia-ficción, pero en un futuro lo vemos más normal

Pero, con toda la seguridad...

Déjale acabar, a ver

Está avisando un poco ese tipo de sistema en la sociedad, te vas habituando

Pues por eso, a lo mejor esto se implanta en un futuro, probablemente se implante y luego nos planteen otras, porque la seguridad sigue fallando, porque cualquier sistema de seguridad tiene un fallo

Que te vean desnudo quinientos metros antes del aeropuerto ¿no?

Cada vez más la tecnología pues irá quitando fallos, que te quiten privacidad, que no te quiten tanta

Antes ponías un ejemplo

Perdona, déjala acabar

Lo que el dice, que cada vez irán un poco afinando

Siempre va a ver un error, siempre que vaya una persona en un sistema, siempre tienen error, siempre puede haber una persona detrás que puede ver un error o incluso la manipulación

Eso también

¿Qué decías tu antes que te han cortado? Estabas diciendo...

Que digo que con toda la que se ha montado en EEUU con el royo del atentado y la seguridad, y un equipo, un equipo de televisión, yo al menos lo he visto en televisión, trataban de demostrar que eran absurdos, se han saltado todos los controles, todos los chequeos, todos los escáner y entraron con unas cómodas pistolas e hicieron fotos y videos en el avión.

Eso viene a corroborar una de las opiniones que estáis manejando que es la de la ineficacia.
Bueno, vamos a tratar de hacer una ronda, da igual el orden, da igual por donde empecemos, pero me gustaría que concretaseis, una cosa rápida, una ronda rápida, los aspectos positivos, (hemos analizado mucho los aspectos negativos).
Los aspectos que podáis considerar positivos de estas tecnologías muy concretas, me refiero a centradas en los escenarios que hemos estado trabajando aquí. Repasamos otra vez, las biometrías, el control de flujo de comunicaciones, los controles por videocámara, el desarrollo de tecnologías que potencian la privacidad, no se, creo que me dejo, si, los localizadores, de los que habéis hablado, y que os parecen positivos por una parte. Darle un repaso a estos aspectos de los que hemos hablado, vamos a ver si en una ronda podemos llegar a concretar ... ¿vale? Vamos a empezar pues por ti mismo.

Yo veo positivo la seguridad ,en cuento a la privacidad creo que se tendría que...

Vamos a ver si logramos, de todos los casos que hemos visto aquí ?

En general

En general, bueno.

Yo en general me parece bien todo, solamente que se utilice bien o para bien.

Yo, por ejemplo hay unas que, la biometría, quiero decir que la estamos utilizando, mi huella es biometría, entonces dentro de la biometría desconozco cual es la lectura y a mi lo del rostro no me gusta y luego las demás, pues circuito cerrado, a veces una cámara me puede molestar, a veces me puede dar tranquilidad, pero yo que se para que me está grabando, luego los localizadores si, como ayuda para accidentes me parece que está muy bien si no se desvían las funciones, luego, conocimiento de la información de eso, de las bases de datos que se puedan cruzar y, yo creo que tiene que estar muy justificado y mejor que sean anónimas y cuando describan algo que con una orden judicial que se investiguen, luego lo de las radiofrecuencias yo es que no utilizo, me da igual, bueno para mi no las utilizo, no, ni creo que las vaya a utilizar. Escáner, la máquina al desnudo pues nada, escáner bueno, si cuando paso por el aeropuerto lo acepto porque me da seguridad, lo que ahora es detectar los metales cuando paso por, bueno a lo mejor que se vea el maniquí ese pues tampoco me molesta demasiado si tengo seguridad. Y luego que más hay aquí, lo de que me intercepten las comunicaciones pues no, solamente lo justifico cuando haya que prevenir algo, pero no en el contenido, sino que cuando ya se tiene un indicio de que hay un peligro de que cuando cualquier cosa en casos de terrorismo o de..., pues que se pueda utilizar

Yo diría que para, cuando viajas pues ahí no pierdes ahí es lo que te vale, ahí una tarjeta o tu huella que no haya lista de espera, esa es una ventaja, pero, es

una ventaja eso, que a lo mejor no puedes esperar ahí, a lo mejor tres horas hasta que pasa alguien

Esa tarjeta vale mucha pasta, esa tarjeta vale mucha pasta, ahí si que va toda la base de datos y que eres bueno, buenísimo y te sacas esa tarjeta, o sea, seguimos con lo mismo, cuestión de pasta.

Vale, tu veías positiva la tarjeta

Yo la veo positiva esa, lo demás no lo veo positivo

Lo demás no.

Yo lo veo bien a nivel general, pero que la que más positiva es la de eCall, la del coche

Yo por ejemplo la biometría, yo estaría de acuerdo siempre y cuando es para algo oficial, el DNI, un pasaporte y cosas así, para otras historias pues no.
Yo por ejemplo lo del reconocimiento de matrícula me parece perfecto y lo del circuito cerrado de televisión ya si que me da igual. Luego lo del eCall me parece muy bien, siempre y cuando sea un accidente coja y se active, no cuando este todo el rato activado porque para eso si quiero me pongo un GPS ¿no?
Luego lo de desviación de funciones, toda las cosas me parecería horrible. Luego el conocimiento total de la información pues no porque me parece que eso es jugar con mas sentidos, todo el mundo conoce a todo el mundo y ya eso me parece muy mal. Identificación pro radio frecuencia me parece bien, bastante bien y lo del pasaporte biométrico y eso. El escáner de pasajeros y lo de la máquina al desnudo me parece horrible, yo no lo haría vamos. La retención de datos me parece mal porque entonces ya cuando retienen los datos y que no se borren ni nada de eso ya, no me parece que puedan jugar con ellos ha hacer lo que quieran. Y ya la interpretación, bueno la intercepción de las comunicaciones me parece mal porque ya, si eres un terrorista o algo así entonces si doy aprobación, pero para nada más, y con una orden judicial por supuesto.

Yo, cuando yo estaba leyendo esto pensé, bueno si ahora yo conozco un caso de una persona que, unos atracadores lo cogieron y le hicieron ir a un cajero con su tarjeta a sacar dinero, el día que no utilicemos tarjetas y utilicemos datos biométricos, a mi de alguna forma me pueden secuestrar, o sea es más fácil, ya no quieren quitártela sino que quieren otra cosa y soy yo, de alguna forma si que también me pueden obligar, entonces es más agresivo porque quieren llevar mis datos y mis datos los tengo yo, mis datos biométricos.

¿Seguimos la ronda?

Lo de que salte para emergencias me parece bastante bien.

La utilización para emergencias

Si. Lo de análisis de conducta como para, no se, no lo veo sentido y los biométricos bueno, bueno los biométricos y el reconocimiento de, estructural o del cuerpo, lo veo con fallos la verdad, no lo veo del todo seguro, en utilización en aeropuertos y en otros sitios bueno, hasta que no lo vea más claro, hasta que no lo den más claro, que son bastante eficaces y que pueden servir para algo no lo veo tampoco muy allá, más bien para emergencias.

Vale, seguimos.

Yo creo que se justificaría claramente si fuera como muy necesario, no como algo de un, o sea, tan masivo, como en tantas aplicaciones, se está pensando mucho en eso y el hecho de, cuando haya un fin realmente que lo justifique. Después el hecho de la percepción de la privacidad parece una cosa que, por un lado estamos completamente invadidos y pro otro lado, después nos van a intentar vender algo para que no nos invadan. Por un lado está ese tema y por otro lado tiene un transmisor para su teléfono que le habla en un idioma extraterrestre que no se lo entiende nadie, nadie va a poder captar, pues mire que anda todo el mundo con la maquinita que le escucha, como de espías, no se que

Yo, básicamente estoy de acuerdo con el uso de estas tecnología por lo que os he comentado antes, porque no me siento involucrada, es decir, por ejemplo, si tienen que pinchar una conversación a un terrorista, insito, decimos terroristas, que me da miedo, pero hay cosas mucho más que me dan más miedo aún, hasta que no lo pinchen no van a saber si está o no está, es decir, gente que caiga, entre comillas, en el camino tiene que haber unas cuantas, pero por ejemplo a mi no vana preguntarme por la operación Malaya, es decir, no van registrando a la gente, o quiero creer que no van registrando a la gente porque si. Entonces, partiendo de esa base y partiendo de la base de que considero que hace mucho tiempo ya que la gente no tiene privacidad, desde el momento que naces ya te están dando un DNI o te están poniendo una, lo diré, una pulserita con un número te tienen localizado, te tiene localizado hacienda, te tiene localizado Movistar, te tiene localizado un montón de gente. A mi no me importaría que me tuviese la policía o un organismo dedicado a ello si en algún momento puede contribuir a la seguridad, pero insisto, porque no creo que se este muy implicado.

Vale. Vamos a ver otra cosa. En este equilibrio, en este balance del que estamos hablando todo el rato, estamos viendo distintas caras del prisma, enfatizando unos aspectos, matizando otros. En este balance entre seguridad y privacidad, ¿en que situaciones?, vamos ha hacer también como un pequeño ranking, ¿en qué situaciones estaríais dispuestos a perder o a ceder parte de la privacidad en la tecnología de la seguridad?. Vamos a centrarnos también en cosas muy concretas. En que cuestiones concretas diríais bueno yo acepto perder privacidad... en este caso y en este.

En situaciones de riesgo.

En situaciones de riesgo ¿cuándo?

Ahora tenemos muy aceptado o parece que lo aceptamos que en un aeropuerto nos dejamos hacer cualquier cosa, pero porque en un aeropuerto parece ser el foco del problema terrorista, pero te puede pasar en el aeropuerto como te puede pasar en Atocha

Es decir, ante la posibilidad de riesgo terrorista. Más cosas

En investigaciones policiales.

En investigaciones policiales.

Asesinatos.

Robos o secuestros también, para prevenir ahí

Robos, secuestros

Asesinatos

Asesinatos

Para entrar y salir de las fronteras españolas y eso, que ahora se tiene muy vigilado y es por los temas de terrorismo, entonces si está bien, yo si lo veo bien.

Por el terrorismo

Por el terrorismo o porque puedas pasar contrabando o cosas así. Y niños.

Si, esas tecnologías yo veo por ejemplo como localizar, muchas veces te pueden servir ancianos, los que se pierden, o se a que pueden, que es muy útiles, pero muy útiles.

Bien utilizadas si.

¿Dónde las veríais bien utilizadas?, ¿cuál sería el potencial positivo?, ¿dónde estarían bien utilizadas? Insistís mucho en esto, en la utilización positiva o negativa, ¿en qué estarían bien utilizadas?

Control de ancianos

De niños.

En caso de accidentes.

En caso de, también puedes tener opción a una tecnología que tu te veas en un momento de riesgo porque a ti te agreden, entonces tu en ese momento, igual que es el móvil, que puede ser ayuda, porque para, cuando tu corres un riesgo de, entonces en ese caso

También para las maltratadas

Si, maltratadas, una persona, violencia con las mujeres

El móvil también podría mejorar mucho porque el móvil es relativamente, es decir, tu te vas a una excursión, te pierdes, en la nieve o en el monte y te quedas sin batería o te llevas el cargador, te vas a una excursión, no te lo enchufas, podría cargarse con energía solar, por ejemplo.

No quedarte incomunicado.

Pues yo por ejemplo, no se, a mi alguien tengo una amenaza y yo puedo ser, en ese momento, entonces todos estos sistemas pueden pedirte ayuda, incluso puedes permitir, incluso

Claro, sistemas automatizados para evitar riesgos

Vamos a ver, otra cosa, vamos a pasar a otro tema y vamos a ir ya cerrando el grupo. ¿Quién pensáis vosotros que deberían estar involucrados en todos los procesos de implantación de nuevas tecnologías de este tipo, tecnologías de seguridad?, ¿a quién? -En esa implantación- ¿a quién habría que escuchar?, ¿quién debería opinar?, ¿quién debería de tener voz a la hora de implantar estos sistemas?

Pues todos.

Todos.

La policía, que son un poco así, fascista, pero la policía porque realmente quien va luego a llevar las riendas de este tema. Van a ser los implicados al fin y al cabo, tu si hay un abuso de autoridad o algo o un abuso de tu privacidad, cuando por ejemplo el tema de Movistar, o sea, nadie tiene derecho a tener su número de cuenta por que sí.

No, que lo tengan

No, pero yo estaba hablando que la niña de una tiendecita de Madrid, no que Movistar

Donde quiero llegar es que

A ver, la policía

Claro, que...

La policía ¿porqué? Porque son los que lo van a utilizar ¿Quién más?

El Ministerio del Interior, que es el que está la policía a cargo de ellos

Claro, bueno, si, evidentemente

Se supone que ahí porque tendrían que llevarlo todo

El Ministerio del Interior

Pero, deberían hacer unas votaciones para que la gente decida

Yo personalmente no iría a votar una cosa así, iría a votar cosas más importantes que no están haciendo referéndum, entonces no creo que eso sea ni viable.

Se puede tantear, se puede...

Ya que te hacen tantas encuestas

Claro

O sea, tantear la opinión pública mediante encuestas o mediante..., vale.

Luego ya también Asociaciones, quiero decir que dentro de esto hay muchos grupos que a lo mejor son más débiles y...

¿A quién mas?
O sea, Ministerio del interior, policía, tantear la opinión pública...

Yo no voy a decir quién, sino quién no

Quién no.

O sea, yo creo que en los bancos no tiene porque tener todos los datos tuyos. El banco tiene que tener mi solvencia económica, si le pido un crédito ver que lo va a pagar y punto, nada más.

Bueno, para finalizar, la participación en este proceso que ha empezado con el envío a casa de la documentación que habéis leído y que ha continuado con la exposición que ha hecho Emilio y con esta tertulia o debate que hemos tenido aquí. Todo este proceso, ha influido, ¿creéis que ha influido en vuestra percepción de estas tecnologías?, ¿tenéis la misma opinión l?, o ¿se ha modificado en algo?, o ¿algo os ha llamado la atención?

Yo sigo pensando lo mismo que ayer

Si, yo también he visto algunos puntos que no había pensado

Por ejemplo

Sobre la privacidad que en algunas cosas pues te quitan, pero vamos

¿los demás?

Yo, había tecnologías de estas que no las conocía, entonces, si las, puede ser que lo que he dicho al principio, que me siento más inquieta

¿Más inquieta?

Si, a mi también me parece

¿A ti también te inquieta?

Como darle más importancia, quizás, a lo que, como comentaba, a lo que uno está habituado y demás, el darle como un poquito más de importancia

A mi tecnológicamente me ha llamado la atención

¿Tecnológicamente?

A mi también me ha inquietado un poco porque venía muy tranquila, luego me he quitado un poco porque lo importante son los fines para los que sean

Yo estoy de acuerdo

En ese punto estáis dos de acuerdo

Yo completamente

Como que uno desconfiaría de los fines económicos, comerciales, no para seguridad solamente sino con un fin un poquito elevado y ese tipo de cosas

Que se tiene que ver primero, eso es lo que yo pienso, antes de aplicarlo

Eso es lo que estamos haciendo.
Bueno, pues por mi parte daros las gracias, si tenéis algo que añadir, si queréis añadir algo y sino, por mi parte, espero que aunque os haya inquietado el tema la reunión haya sido grata ¿no?

La verdad que si

Interesante

Ha sido interesante y grata por tu parte

Bueno, pues muchas gracias.

Group 4

A partir de todo esto ... ¿Qué es lo primero que os viene a la cabeza?

Que es muy difícil contentar a todo el mundo, ¿cómo se llega a compaginar seguridad y privacidad?
(se corta)
La seguridad es necesaria. Incentivar con beneficios a los aeropuertos el que los quiera, el que se coja una cola rápida o sino un a lenta.
(se corta)
Habría que potenciar el tema de protección de datos, pienso que sería el camino, dificultades, o sea, premios o castigos.

¿Premios y castigos?

Hombre tanto como premios y castigos

No, premios el que se acoja a eso pues que pase por una cola rápida o sino por una cola lenta. Porque está claro que después del 11-S la seguridad es necesaria

Entonces todo el mundo iría por lo fácil ¿no?

O depende porque si tu quieres privacidad y no quieres dar tus datos

(Hablan a la vez)

A ver, a ver, que hemos dicho que todos a la vez no. ¿Vale? Decías tu...

Yo pienso que tiene que ser a todos o a ninguno

No, no, no, entonces ya me estas violando tu privacidad, yo tengo que tener...

No, pero con respecto a lo que el está comentando, digo, yo estoy de acuerdo en unas cosas y no estoy de acuerdo en otras, pero con lo que el está comentando, en ese caso concreto de lo del aeropuerto

Ah, ¿o todos o ninguno?

Si esto de el que quiera que se amolde a esto y el que no que se amolde al otro, pienso que no funcionaría.

Yo entiendo que no ha dicho eso, yo entiendo que dice que quién se beneficie de las normas

Tenga un incentivo

Exacto. El ejemplo es muy claro, es como lo de la tarjeta de prepago en las autopistas, tu ves que hay una cola y que pasan unos tíos rapidísimos, pero tu has dado eso. Lo que pasa es que la privacidad es, por lo menos yo creo que el usuario hasta ahora, y esto es lo gran sorprendente para mi en esta reunión, es que no hemos pensado en todo lo que significa, el estar, porque a mi la primera opinión que me ha dado la reunión esta es decir, horror, horror, horror.
(risas)
¿a dónde vamos?, a dónde vamos, es que ya no hablemos de privacidad, no va a existir la privacidad. El futuro es sin privacidad según vamos.

Si

Los programas que salen parece que estábamos leyendo a Owen que es de hace veinte años

Claro es de las novelas de hace

Y cada vez más, controlaba todo (no se oye), es una impresión de la preocupación que me produjo

Pero yo creo que ahí está la separación de al privacidad porque cuando tu quieres, si entras en Internet y te metes en una base de datos porque quieres a lo mejor que te hagan un regalito, si te apetece pues tu metes tus datos, si no quieres no lo metes.

(Hablan a la vez)

Depende de cómo sea el incentivo pues...

Pero que siga habiendo esa privacidad

Que lo dejen muy clarito para que se va a utilizar y que tu sepas para que se van a utilizar tus datos

Y que te dejen decidir si tu quieres esa privacidad o no la quieres y que sepas que te están dejando ese espacio. Es que yo al leer eso también me horrorizaba el pensar ¿cómo sigamos así? nosotros no vamos a tener privacidad ninguna

Cuando se viole la privacidad que sea en última instancia un juez el que lo decida, el que lo autorice con un tiempo, con una forma y con los medios adecuados, pero que sea el juez.

Si

O varios, porque yo uno solo como que no se que deciros ¿no?, casi prefiero, hombre, todos somos humanos y todos tenemos errores, si ese señor está ahí puesto y se magnífico no quiere decir que tenga un mal día, entonces prefiero que haya un par de ellos o tres, de verdad

¿Qué mas?
Y si nos ceñimos a los casos concretos de los escenarios que se han planteado aquí, los distintos escenarios de aplicación. Ciñéndonos a cada uno de los casos ¿cómo lo veis?, es decir, que valoración hacéis de cada una de estas aplicaciones.

A mi la que me parece muy interesante es la de eCall, la de los automóviles, pero que tu la puedas activas, es decir, que no te estén persiguiendo. Que cuando yo tenga un accidente diga "poom", salte, pero no que me tengan vigilada de todo mi recorrido, sino para, me parece interesante

Entonces solamente funciona para un caso porque ahí habla de otro caso, el eCall también funciona para robos no en caso de accidente

Bueno, si, pero me refiero el caso, yo estoy utilizando mi coche, que no me estén vigilando, que solo se utilice en el momento que yo quiera, en ese momento, o sea darle de alta. Lo que dices tu, que si le roban el coche no lo voy a localizar.

Claro

Puede ser, también

Son buenas para unas cosas y son malas para otras, si yo doy mi consentimiento para que me pónganle eCall vale, voy a estar vigilada, pero a la vez si me roban el coche puedo conseguirlo antes, tengo a un terrorista que se mete en el, yo que se, para ese tipo de cosas lo veo genial, pero a ver, cómo llegas a un acuerdo de qué es lo mejor y qué es lo peor. Es que es complicadísimo. Es difícil ponerte a decidir.

Es que todos, yo creo que hay pros y contras

Tu no te referías a eso cuándo has preguntado

Hemos empezado hablando en general, habéis hablado en términos generales y yo lo que os pedía ahora es que tratásemos de concretar, en los distintos escenarios que aparecen en el texto que os hemos enviado ¿qué valoración le dais? O ¿lo veis igual?, ¿establecéis algún tipo de diferencia entre las distintas aplicaciones? esa es un poco la pregunta

Pero estáis hablando en cuanto a la postura de los dos casos específicos en, de los dos ejemplo, dela tal señora esta

Si, de los ejemplos

Bueno, pues ahí hay dos, el de la señora es opcional, ella se da cuenta que, me parece, que elige, pero el otro elige sabiendo lo que significa, acogiéndose a las ventajas de todas esas cosas. Lo que pasa es que

luego hay una cosa curiosa y es que la señora no sabe que el hijo la está controlando y eso es una paradoja y entonces, si, vale como ejemplo.
Aceptamos, pues si aceptamos, según que casos, pues en los casos que nos sean favorables, casos que tu pienses que tienes ventajas con ellos ¿no?. ¿En qué casos te fastidian?, pues en los casos en que se meten en tu privacidad y llega aun límite, no se.
Y luego existe el riesgo de todas las confusiones posibles que pueda haber, en los fallos de maquinaria que pueda haber, en todas esas cosas que pueden complicar la vida

Yo creo que todos hemos oído que le han metido en el RAI por equivocación y le destrozan la vida y luego era mentira, era otro que se llamaba igual, era...

(Hablan a la vez)

Es el precio que tienes que pagar para tener tanta seguridad, si tu aceptas eso pues tienes que aceptar que te puede tocar eso. Pues eso, estás de acuerdo, si estás de acuerdo tienes que saber que te puede pasar eso o que no.

Pero ¿tu estás de acuerdo con todo lo que ahora mismo pasa?

No hombre, no

Que hay cosas que te las han impuesto y te las imponen y estás diciendo que tienes que entrar por el aro, porque ahora hay cámaras. Pues imagínate que aquí hay una cámara, a mi se me ha ocurrido al entrar, ¿oye aquí hay cámaras?
(Risas)

No hay, no hay.

Se me ha ocurrido.

Pero podría.

Pero podría haber.

Es que la imposición de todo esto... . Digamos que el ciudadano se tiene que defenderse de muchas imposiciones.

Pero tu aquí has entrado preguntándolo con lo cual tienes la posibilidad de decir, ah que hay cámaras, pues me voy.

Claro

Lo malo es donde no tienes esa posibilidad.

Claro, es como lo de la señora, la de la tal Carla que no sabe que su hijo la está vigilando. Ella llama para decir que llega bien y el hijo dice bueno, vale.

Ya lo se

Pero es que yo creo que estamos más vigilados de lo que nosotros nos imaginamos, que es lo triste, o sea que, yo creo que tendría que haber muchísima más información de todo este tipo de cosas de tecnologías de seguridad

¿Quién tendría que dar esa información?

Pues dependiendo, pues me imagino que...

Quien autoriza, quien autoriza esa...

Quien las imponga en ese momento

La de la protección de datos

Si ponen cámaras que avisen

(Hablan a la vez)

Quién las imponga

Por seguridad que te digan que te van a vigilar, pero que lo avisen

Es que el que no tiene nada que ocultar, a mi no me molesta

A mi particularmente tampoco

Depende de tu...

(Hablan a la vez)

Todos a la vez no

A mi no me molesta

A mi tampoco

Hay dos que opinan que no molesta

Es que yo pienso que si no haces nada malo, es para tu seguridad si alguien te va a robar, pues no se

Me molestaría lo del aeropuerto, lo de los rayos x estos, eso si me daría un poco de cosa, peor por ejemplo con el otro método, el del maniquí

pues no tendría ningún problema y mucho mejor, así nos evitaríamos estar, que si el móvil, que si las llaves, que si lo otro
Te pueden hasta robar la bandejita, te pueden hasta robar las llaves, el móvil. Pero bueno, en un banco por ejemplo yo lo veo genial, que haya cámaras, cuanto más mejor y en ciertos sitios también lo veo muy bien, al verdad. Hombre lo que pasa que por ahí la calle, tampoco, no se. Yo pro ejemplo pienso que en los portales debería de haber alguna.

¿En los portales?

Si. A mi me han atracado en el portal de mi casa y mira, lo pienso desde entonces, si hubiera aquí una cámara pues por lo menos

Lo que pasa es que hasta que punto todas esas cámaras están, te quiero decir, en el portal, ¿hasta que punto esa cámara está realmente conectada?, o sea, ¿van a venir rápidamente ayudarte? o ¿cómo?, ¿para que va a servir realmente?, ¿Hasta que punto eso es bueno?

¿Qué creéis?

Pues que eso queda ahí como prueba

Es que no lo se.
Si, pero yo no quiero una prueba a mi me han robado, a mi me han hecho daño, yo no quiero esa prueba, yo quiero que en el momento que me vean

Pero si la persona que te ha robado está fichada pues se puede...

Pero es que yo quiero que no me llegue ni a pasar

Hombre, pero eso es lo ideal

Yo quiero que me vean de verdad, que si me va a pasar algo que alguien venga a auxiliarme. Para eso, si que no me importa perder mi privacidad. Ahora, si voy a quedar ahí gravada, voy a ser la caso ocho mil no se cuantos y cuando le cojan a el va a estar dos meses y va a salir pues, no se hasta que punto. Hombre, vamos a ver, evidentemente en su momento me va a alegrar, pero me gustaría que fuera algo más, que realmente que sirvan de algo, que sea algo más...

Que haya más seguridad.

Si.

Por ahí estaríais apuntando a una posible ineficacia. O sea que habéis apuntado al aspecto invasivo, pero luego al mismo tiempo a...

Es que si hay tantas cámaras no puede haber tanta gente detrás de ellas. Eso estará localizado en algún sitio, pero claro donde, te quiero decir, si hay veinte mil cámaras detrás de un edificio no creo que haya veinte mil

personas detrás de cada cámara, no, habrá un sitio peor dependiendo de donde este. Si hasta llegar a donde estoy hay diez kilómetros, de qué me va a servir casi esa cámara. Si, que queda grabado y luego vale, no queda impune lo que pase, pero

Pero esta cámara de por si es un elemento disuasorio

Si, también es eso

En un garaje pone, garaje vigilado por videocámaras, eso es disuasorio ya

Si.

Solo el hecho de que haya cámaras. Las cámaras como tengan, las hay activas y las hay pasivas

De hecho las hay falsas.

Ahí quería llegar, que hay tantas que, vamos yo he oído comentar a las personas, esta será falsa, esta no sirve para nada. Entonces claro, no sabes si eso realmente te sirve para algo o no.

Yo soy partidario que haya cámaras donde se quiera siempre que se avise que hay cámaras. Si una junta de vecinos decide ponerla en el portal me parece estupendo, que decide en la parte de la calle, me parece estupendo, pero siempre que se avise

Sobretodo también para ver quién destroza el portal, para ver quién rompe el cerrojo, a ver quién ha roto la cerradura y eso porqué, pues ya se pone una cámara y así se coge a quién lo está haciendo porque es un fastidio para toda la comunidad

O ya no lo hará, como sabe que está vigilado

Claro, pero es que vamos

Bueno, estáis poniendo ejemplos... y enlazado con lo que decíais antes de que es un precio que hay que pagar, como has dicho tu, o que en parte beneficia; pues en esta tónica de ejemplos que estáis poniendo, estas aplicaciones que hemos analizado hoy, ¿en qué casos concretos os aportarían beneficios o serían positivos?. Estáis hablando ahora en concreto de la video vigilancia y habéis puesto algunos ejemplos donde sería positivo, os favorecería o compensaría. Pues vamos a seguir por aquí, en...

En el metro

En el metro.

Asegurar que es eficaz en el sentido de que hay una conexión directa y que se puede intervenir, que vaya más allá del efecto disuasorio o considerando el efecto disuasorio como importante.

Es importante

Es importante, vale. Esas serían unas cuantas aplicaciones de esta aplicación concreta de la tecnología de la seguridad que sería el video control, ¿qué más?, no se, por ejemplo, la biométrica. ¿Qué aspectos?, ¿qué potencial positivo tendría para vosotros?, ¿qué aspectos podríamos pensar que es positivo?

A mi utilizarla sobre todo en los aeropuertos

Digo esto como ejemplo, si queréis coger otra...

Si. En los aeropuertos

Es que en otro sitio sería excesivo.

Si

(Hablan a la vez)

Para que no te confundan.

Yo lo que haría es que se hagan un poco más seguro los pasaportes, porque es que ahora mismo no son seguros.

Lo que pasa es que a mi me da un poco miedo lo que nos comentaban que te roban la identidad, eso me parece un poco como inseguro, que parece como una herramienta muy segura, pero que te roben la identidad, eso me parece ya como muy fuerte, me horroriza. Que esa persona pueda impunemente hacer lo que sea contigo y que eres tu

¿Contra eso no hay nada? No hay, como el que hizo la ley hizo la trampa, ¿no hay algo que a su vez te asegure un poco más de?, ¿no?

No se, yo estoy como vosotros

No porque si ya de primeras, no se si se estará poniendo ya ese sistema y demás, y te dicen eso, es que hay una posibilidad sino la ponen como mucho más segura. No que siempre hay alguien detrás que pueda involucrarse y meterse en todas partes, igual que las tarjetas de crédito y tal, la seguridad al final es como relativa. Que te quita parte del riesgo como nos hablaba Emilio, pero deja, lo deja un poco abierto.

Todo el tema de bases de datos cruzadas, ¿cómo lo veis?

Yo, si se hace un uso bien lo veo bien, pero a mi me molestaría que lo utilizara una empresa privada...

Y que te estén machacando

Si, y eso, porque si es con fines comerciales es una pesadez,

¿Qué sería?, dices, mientras se haga un buen uso ¿qué sería un buen uso?

Utilizarlo para el fin, si se ha dado para una encuesta que sea para eso. Que tengas siempre acceso a borrarlos, a rectificarlos

Pero, ¿cómo lo veis cuando ese sistema se aplica a temas de seguridad?

Bien, yo si se aplica a temas de seguridad bien. Lo malo es, o sea si vas a por algo que es sospechoso y estás seguro y te ha seguido sus pasos, su red y vas a por toda esa gente que ya tienes como sospechosa bien, lo malo es cuando, porque si me acerco y cojo un poco más del ámbito de alrededor de esa persona, que a lo mejor no tiene nada que ver. Entonces ya estás sacando, te estás ya pasando. Siempre que se aplique al sospechoso me parece estupendo.

Eso tiene que estar bien organizado, por el Estado, por

Debería

Debería estar muy organizado y por la Comunidad Europea, que no estemos siempre dependientes de lo que diga EEUU. EEUU dice voy a (no se entiende) y todos voy a, no hombre, no. Yo creo que esto lo tienen que aceptar, más que los Estados, incluso las Comunidades e incluso la Europea, pero tiene que estar regularizado con directivas muy estrictas y que solamente, yo creo que esos confederados se puedan hacer en un momento determinado autorizando por sistemas judiciales o por sistemas oficiales, no se. Yo creo que aunque, auque el que hizo la ley, hizo la trampa, hay que hacer la ley de todo esto para que por lo menos la trampa se haga menos, la ley es un elemento ultrasorio simplemente.

Cuando hablamos de regulación , os estáis refiriendo en concreto al tema de bases de datos cruzados

Si, si claro.

Bueno en todos los aspectos, hay que regularizar absolutamente en todos los aspectos, no se, yo creo que vamos por detrás de ¿no?, el tema de protección de datos surgió cuando tu tenías dado tus direcciones y tus NIF a doscientas mil personas que la usaban ya, al salir la ley de protección de datos y luego sale ahí en los papeles con una letra chiquitita que tu no te molestas en llamar para que no te llamen a las tres de la tarde. Entonces yo empleo elementos disuasorios para eso, yo por

ejemplo cuando llaman preguntando por mi mujer para el teléfono digo, yo le digo que me he divorciado con lo cual pasa y ella dice lo mismo, le digo que me he divorciado, que no vivimos juntos y pasan, con lo cual la base de datos...

Pues hay muchas personas que trabajan, hay muchas personas que trabajan en ese tema ¡eh¡

Pues que trabajen, si a mi me parece muy bien que trabajen y que pidan esos datos, a mi me parece muy bien, pero yo estoy alas tres de la tarde descansando

Tu imagínate que trabajas en lo mismo

Pues a lo mejor habría que buscar otro puesto de trabajo diferente, ¿entiendes lo que te digo?, no se, te quiero decir que tu no tienes, tu que haces la encuesta no tienes...

No si, que lo entiendo, que lo entiendo

Además es que te llaman siempre a las tres de la tarde

Y a la hora de la siesta

Me llamaron antes de venir aquí y ya dije que no que llama otro día que ahora no puedo

(Hablan a l a vez)

De todos los aspectos negativos que venís mencionando ¿cuáles son los que más os preocupan?, o sea, ¿qué es lo más negativo?

Pues que te dejen sin privacidad, es que. Que no puedas hacer nada sin que estés controlado que vayas donde vayas

No tener libertad

Más que controlado manejado, ¡ojo¡

(Hablan a la vez)

A ver, aquí introducen un matiz, el de la manipulación ¿cómo sería?

Manipulación en cuanto que tenemos, sabemos que todo esto es muy bonito, está muy bien y los Estados te van a garantizar, pero que no se sabe nunca cómo pues, las empresas, entidades, capital, se apodera de esos datos y caes, no se, manejan, te van a manejar, no se, hasta tus apetencias

O sea que sería una manipulación de tipo comercial

Si, claro. Bueno comercial o puede ser más cosas

¿Cómo veis esto?

Yo creo que se puede saber todo de una persona, si, escuchando las conversaciones, mirando las páginas que visitan, entonces eso, vale a mi me parece bien, pero que sea alguien capacitado para ello, que no pueda verlo cualquiera. Que no pueda haber un uso de esos datos

¿Cuál sería esa capacitación?

Yo para mi es el juez, o sea

El juez
Pasaría, como habéis dicho antes ¿ pasaría por la visión de un juez? ¿si?

Pero el juez, anteriormente tiene que tener una regulación

Si, efectivamente, una ley

Porque ahora mismo, muchos de esos casos y lo estamos viendo los jueces están dictando sentencias por bueno, casos técnicos de estos y no saben de que van.

A la hora de implantar este tipo de sistemas, ¿a quién habría que tener en cuenta?, ¿a quién habría que escuchar?, ¿quién tendría que estar involucrado en estos asuntos?

Los ciudadanos sobretodo.

Los ciudadanos sobre todo

Porque son los que más van a sufrir las consecuencias de ello, tanto buenas como malas

Pero ¿cómo?, ¿a través de qué?, porque claro el ciudadano, ¿pero a través de qué?

Es complicado

Tipo referéndum, es que a ver como te pones de acuerdo de todos los gustos y d todas las cosas que quiere la gente. Pues lo que te digo, tipo referéndum.

A través de un cuestionario

¿De un cuestionario?

Si. Estadísticas.

Estamos en ello ¿no?

Yo creo que con la información los movimientos ... salen con información. Información de los países o de las comunidades o de quien sea, información de la implantación de todo esto.

Informar al ciudadano. Al ciudadano a través de los medios de comunicación

Claro, dónde vas a informar. No te sacan esto que es un rollazo.

Pero sobre todo de...

No, es que al final no se lo iban a leer, realmente no.

Los políticos son los que tienen que informar de todo esto

¿Los políticos serían?

Claro.

O sea, los ciudadanos deberían participar a través de información de...

A través de Asociaciones de consumidores

¿Asociaciones de Consumidores?

Claro.

Empresas de seguridad, pero no ellas solas, claro, también tienen algo que decir pero no todo.

Las empresas comerciales no tienen nada que decir en esto

¿No?

Yo creo que no.

O sea, que sería más bien...

Los ciudadanos

El gubernamental, el gobierno. Pero luego es lo de siempre, quien está aquí a lo mejor está más interesado en este tipo de seguridad y el otro en otros y...
(Hablan a la vez)
Siempre habrá muchos intereses creados, yo creo que es un poco

Yo creo que habrá más gente en contra que a favor me parece, me da a mí

Por el tema de la privacidad, que sea seguridad y te lo vendan como seguridad, pero la privacidad.

Si, me puedo equivocar, pero

Creéis que si se hiciese una encuesta mayoritaria, la mayoría estaría en contra de este tema

Yo pienso que si fíjate.

Depende de cómo lo plantees, si te lo plantean como un tema de seguridad, como terrorismo seguramente que estarías a favor, pero si te lo plantean de otra manera y el uso que vaya a tener

... para la seguridad

pero es que si te lo empiezan a vender a partir de ahí

Depende de cómo te lo planteen

que es para ti mucho más seguro, que vas a poder viajar mejor, llevar a tus hijos al colegio, que tu al final sabes que no te va a pasar nada, siempre, tu coche, no se que, si te empiezan a venderlo por ahí posiblemente haya más gente que diga que si

Aún así la gente somos muy cabezotas

No, nos da miedo lo nuevo, lo que no conocemos, eso es lo peor. Yo creo que costaría mucho ir implantándolo porque las cosas que no conocemos nos asustan, pero es normal. Pero tu empezarás a ver como iba aquello, como realmente servía para lago y si realmente era fiable y me servía para mi seguridad, hasta que eso no se empiece a ver

Que realmente se demuestre, que es así

Y que no tiene contra..., que no va a ser, que no es contraproducente

Vosotros, en este dilema entre privacidad y seguridad, en que aplicaciones estaríais dispuestos a perder algo de privacidad, algo, mucho, poco de privacidad para conseguir mayor seguridad. ¿En qué cosas?

¿En la vida diaria?

Si. Decir, yo en esta aplicación acepto perder privacidad porque gano seguridad ¿en qué casos concretos?

En el metro, por ejemplo.

En el banco, en el metro.

En el aeropuerto.

En el aeropuerto.

Transportes públicos.

En el autobús, hay pienso en el señor que conduce que si pasa cualquier cosa...

Portales

En los estadios no se yo

También, también

En los locales públicos, pero

Donde pueda haber terrorismo

Donde pueda haber masificación

(Hablan a la vez)

Donde pueda haber terrorismo

Masivo, si, eso. Y por supuesto en los sitios comerciales, pues que quieres que te diga

Pues también

El que por una máquina puedan ver si yo llevo una pistola o no, pues a mi me darían muchas garantías y podría ir yo con mi familia tranquila

Claro

¿En algún aspecto más? ¿En algún ámbito más?
Antes, al principio hablabais, cuando hemos empezado, en la introducción, al principio, hablabais de los coches, para el tema de control de accidentes ... ¿Eso?

También, yo creo que en el coche también es.

Yo lo veo muy bien eso, o sea, yo lo veo complicado que se pueda, pero que se pueda activar, voy a viajar me lo activo, tengo un accidente con el coche, pero que me den la oportunidad de activarlo.

O el querer llevarlo o no llevarlo.

Que no te vayan a poner una multa por llevarlo desactivado, claro, que tengas opción.

Perdona no te he oído, hablabas ..?

No, que puede ser que tenga contradicciones porque los terroristas pueden utilizar eso y decidir no activarlo y sigue siendo un terrorista. Entonces, ahí está también, si decir que si todos o no, o opcional

Es que es complicado

(Hablan a la vez)

es que no van a dejar de utilizar un coche, pero se proveerán de otros medios para no dejar rastro

Claro, yo lo veía como un tema más, como el que tienes tu de positivo para ti, como una cosa más positiva parta ti, no tanto como para el tema del control de la seguridad, del terrorismo y demás, yo eso no lo vería muy enfocado a eso, enfocado para ti, para tu beneficio

En esto pone que unos terroristas fueron detenidos en Alemania por este sistema, pero pienso que sería la primera vez, en cuanto esto se propague no va a volver a pasar. No lo van a volver a coger a terroristas, por desgracia

Antes, habéis hablado de la necesidad de regulación, ahí también hay un pequeño conflicto, entre si se debe regular el desarrollo de estas tecnologías y por tanto limitar a las empresas, antes habéis mencionado a las empresas o claro, el dilema es poner freno a ese desarrollo, o por el contrario, dejar libertad, dejar libertad para que sigan investigando, para que sigan desarrollando, no estoy hablando ya de la implementación sino del propio desarrollo, este aspecto ¿cómo lo valoráis?

A mi que siga el desarrollo me parece interesante. Que se vayan viendo cosas nuevas, pero luego con unos límites, o sea, que luego se pueda regular y que diga, bueno hemos descubierto esto y que luego se pueda o no implantar dependiendo de lo que pueda perjudicar pues eso, a la privacidad de las personas.

O sea, que debería haber como dos...

Un control

Pero luego que se regularice

Y la regularización ¿por parte de quién debería...?

No se, comisiones parlamentarias, pienso yo, el parlamento

Comisiones parlamentarias, el parlamento que se yo. Los Jueces

El ciudadano también.

Si, el ciudadano también.

A través de organizaciones de consumidores, a través de juntas de vecinos, no se, cosas así.

¿Algo más?

No, la investigación tiene que estar abierta siempre

Es positivo

Claro, siempre que se saquen cosas nuevas

¿Quién se podría pensar qué se podría identificar a una persona por el iris del ojo hace años?, me parece que es importante, pero claro, tiene que estar canalizado, naturalmente. Porque sino vamos a ser numeritos

¿Vamos a ser?, perdón

Numeritos, que ya somos

Ya somos, antes de entrar aquí a parte de nuestro nombre nos han pedido

nuestro carnet de identidad, entonces

Si, pero no te ha dicho que enseñes la patita

Hombre, no creo que llegue la cosa a tanto

¿No? ¿Por qué?

Porque yo no creo que esto llegue a esas cosas

Yo si

Yo creo que si

Yo pienso que al final no

Quizás tu y yo no lo veamos, pero, tenemos cierta edad, no será de inmediato, pero nuestros hijos

¿Tu pensabas que hace veinte años ibas a tener un aparato en el que estabas localizable en todo momento?

Ya, pero lo de las cámaras sobre el control de las personas, eso lo veo más difícil, aunque sea para los casos del terrorismo

¿Porqué lo ves más difícil?

Pues no se porque lo veo, por lo menos aquí en España, lo veo

¿Por qué?

Pues no se, porque yo pienso que la gente no va a estar a favor, que va a ser eso un proyecto muy difícil, muy complicado para ponerse todos de acuerdo, no se. Yo desde luego cuando he leído los papeles he pensado, uy esto no, vamos que no creo que llegue a , se puede hacer algo, pero no creo que llegue la cosa a tanto, o se, no se

Pues yo creo que está a la vuelta de la esquina, vamos

Yo también

(Hablan a la vez)

Pero es que esto, por ejemplo, lo que tu comentabas del móvil, todos estos adelantos que hay ahora, a ti no te quitan tu privacidad, tu sigues teniendo tu privacidad ¿no?

No, cuando te llaman ya te están localizando

Ya vale, pero te estoy hablando en tu entorno, pero de cara a fuera, pero que llegue al control ese, pim pam tanto, no

¿Cuál sería el control pim pam?

(Risas)

Bueno pues eso, el control ese tan exhaustivo que quieren, tan exhaustivo, ¿no?, por que me parece demasiado, eso, ¿sabes? , por eso te digo
Ahora por ejemplo los bancos claro que ya lo hay, solo hace falta que pongan más y por mi encantada. En los portales, en el metro, en esos sitios vale, pero todo eso de ya, pues eso en los probadores de mujeres, en los…

Eso ya no

A mi me pasó una cosa curiosa una vez y es con lo de los bancos, yo soy un desastre y me dejo muchas cosas por ahí y tal, y estaba en un cajero y estaba como con la cartera, no se que y saqué cien euros y entonces me fui y cuando, había un apersona detrás, y me fui y cuando voy a echar mano al dinero digo, si no he cogido el dinero, me habría pasado ya otra vez y cuando pasan tres minutos el cajero automático devuelve el dinero de nuevo

Si se lo traga

Pero en este caso

No lo tragó

No, entonces yo fui al banco a decir que ya que había una cámara que estaba ahí, ¿quién era la persona siguiente, qué tarjeta había entrado y tal? Y me dijeron que era prácticamente imposible. Que era muy difícil, que no lo sabían. Me quedé sin cien euros y había una cámara ahí. Esto es un caso curioso, que lo cuento como anécdota y no tiene importancia.

Como que no la tiene, la tiene, la tiene

Está en la línea de lo que ella decía

Claro

La tiene mucha porque no…

Yo presencie un robo en el metro de un carterista y el hombre dice, menos mal, menos mal que hay cámaras, fue a consultarlo y las cámaras solo ven, no grababan, con lo que se quedó el hombre hundido. Si alguien estaba mirando le habían visto, pero sino no grababan, o sea.

Os digo que las cámaras hasta cierto punto, claro. Si sirven para algo y van a grabar y hay alguien detrás que te pueda ir a apoyar y como en tu caso eso está grabado y ves a ese señor, estupendo

No fui una vez, fui varias veces

Pero ya has visto para lo que te sirvió

Nada, para nada

Dicen que hay, yo he oído comentarios, lo que pasa que no me he enterado de lo que es, que se, o sea que ponen como una cámara ¿no?

Y te duplican el número

Si con tu número de tarjeta y te

Lo ves, encima eso, eso es la contraposición

No me he enterado

Hay una aparente contradicción porque por un lado planteáis cierto temor, bueno cierto temor no, un temor claro ... a la invasión y a los procedimientos invasivos, por otro lado reclamáis más ... eficacia...

Pero esto es como el señor que va al Hospital y quiere lo último de lo último, o sea, que me tengo que operar y tienes una tecnología punta que además me va a venir genial y voy a curarme en dos días, Dios mío ponme eso y no me apliques el rajarme en hasta arriba y el tenerme un mes en la cama, es que queremos lo bueno de las cosas sin que haya contras detrás

Ya que me retrata, es decir, que sirva para algo

O sea que sería…

Ya que me ven con una cámara que sirva para algo, efectivamente, que no esté ahí para nada.

Bueno, decías alguno que cuando habéis leído esto os parecía un poco Gran Hermano, Orwel y cosas así

Si a mi me lo ha sugerido y hace mucho tiempo de eso

¿En que medida el paso por esta reunión y los precedentes de la documentación enviada y la charla de Emilio y el cuestionario, influyen o han modificado vuestra percepción del asunto? ¿ha mejorado?, ¿ha empeorado?, ¿hay algo que os ha impresionado más?

Yo es que pienso así, yo pienso que esto va a llegar y como creo que va a llegar y no tardando demasiado, no me ha impresionado demasiado, o sea, si que el biométrico ese no lo había oído en mi vida y me ha dejado un poco así, pero por lo demás creo que está aquí a la vuelta de la esquina.

Yo creo que la ha mejorado porque nos hemos dado cuenta de muchas cosas que no teníamos ni idea de que existían y que, pues más tarde o más temprano tienen que llegar

O sea que os ha interesado, decías tu

Si, que yo me he interesado más, me enterado de cosas que desconocía y ahora estoy más interesada

Hombre, son muy importantes y luego el debate. Esto está dentro de las iniciativas que hay que tomar para estar informados, aunque sea investigaciones sociales o socioeconómicas, como tu quieras, pero a mi me parece importante y yo he aprendido. Me he dado cuenta de un detalle que tampoco quería tener, a mi esto que más me da, me parece que no haya atentados y que no me atraquen es importante, pero lo que se está haciendo por todo esto pues no lo sabía mucho

Y tu decías

A mi me parece estupendo, yo muchas veces lo he pensado, a lo mejor, aquí tendría que haber una cámara, no se que, yo muchas veces o he pensado, así e ocasiones extrema que me he encontrado, que he pasado miedo, que tal ¿no? Pues si, si y me parece estupendo la verdad, me parece muy bein, sin llegar a ser tan así

De todas formas, habéis dicho antes que ahora me acuerdo y que yo no estoy de acuerdo en absoluto, decís por ejemplo, poner cámaras en los portales, pues yo te digo una cosa, en los portales la comunidad de vecinos no tiene que tomar la postura de la policía, o sea no tiene que hacer de policía, la comunidad de vecino por otro lado, pero si eso se hace como obligatorio como van ha hacer otra serie de cosas y por decreto ley pues me parece bien, que los portales estén dotados con una cámara, me parece bien, pero que nosotros mismos nos impongamos el control, me parece un poco absurdo

Si lo malo no es el control, es por ejemplo e ese caso, en el caso en que te vayan a atracar, por seguridad, ya se que tiene dos vertientes, pero…

Pero ¿que la comunidad de vecinos va a velar por eso?

Ahí está ¿quién lo va a utilizar?, es la utilización de esa cámara

Yo concretamente me fui de una comunidad de vecinos

Porque estaban muy vigilados

No, porque iban a cercar y a poner cámaras, os lo digo hace ya quince o diez y siete años

O sea que ya en vez de mejorar la cosa lo que querías era que se quedara…

No, yo quería vivir

Tranquilo

Iban ha hacer un aparcamiento subterráneo y un montón de cosas y yo me fui. Ahora contado así parece un poco, pero si

Y por ejemplo roban en…hay perdona

Es que tu decías que sepan con quién entras y con quién sales

Claro, es que te sientes controlado porque dices, bueno están viendo con quién entro a casa, con quién salgo, entonces siempre habrá pues pros y contras

(Hablan a la vez)

Pero eso no se va a exhibir en un cine, con quién has entrado o no has entrado. Eso es un esto que se queda guardado por si ocurre cualquier cosa.

Y ¿quién lo ve?

Tu dices que no importa porque la gente…

Porque es un vecino o un amigo, la gente no te conoce de nada, te da igual
(Hablan a la vez)

Depende de cómo se utilice, porque si está ahí grabado y cada x tiempo se borra

Yo no lo veo problema

Y que solo se vea en concreto por un caso, porque un vecino quiera ver en ese momento por lo que sea, pero porque alguien lo solicite, no así alegremente porque uno este visionando todo lo que pasa ¿no?

Tu imagínate te vas e vacaciones, entrar a robar en tu casa, entran a robar o roban en tres casa y qué, y nadie sabe nada, nadie ha oído ruidos y nadie sabe nada, por lo menos oye, se ha visto que personas ajenas a la comunidad, a lo mejor ha sido el vendedor de yo que se, del supermercado que.. ¿entiendes?

Bueno, pero que se vean casos puntuales

Claro, claro, porque eso no sería un Gran Hermano, por la noche pones la televisión y ves todo lo que ha pasado en

(Hablan a la vez)

Perdona, no se te ha oído

No, pues eso, que abriría muchas cosas de ver con quién ha entrado, no se que, es para ver casos puntuales, entonces para esos casos sí, pero como que para los demás como que no.

Pero no se exhibiría, no sería de dominio público.

Pero también habría que poner quién lo ve y una persona…

¿Quién lo ve?

Ahí está, desde luego un vecino creo que no. Creo que debería ser, no se, un vigilante, alguien que tengas para ese fin

Un conserje

Un conserje, alguien que este para ese fi, punto. Y que luego se borrara, claro, si no hay nada, si no ha pasado nada en esa semana que pueda. Bueno en vacaciones y tal habría que durar algo más la cinta, por si acaso encontrabas algo más

Pero que no nos establezcamos como policías, que el ciudadano que vive en una casa no tiene que vigilar, tiene otros derechos, tiene unos derechos, hay una policía que te protege, hay una ley que te protege, no

Pero no siempre está ahí, ese es el problema

Madre mía, bueno

No siempre está ahí.

Es como una seguridad

Claro, es que

Yo lo veo como una seguridad y disuasorio, como hemos comentado antes

Perdona, ¿dices?

Pero si te roba la casa pues tendrás que tener por ejemplo, pistas utilizando esas cámaras para poder ver quién te ha podido robar, porque si nos ponemos así en que no podemos poner cámaras, entonces nunca se va a poder averiguar quién ha hecho esas cosas, quién ha robado en las casas

O quién ha destrozado las puertas

O quién ha pintado en la fachada

O quién hace pis en el portal todas las noches y no es el perro. Quién rompe los buzones. Es que hay casas que…

Ya, ya, ya lo se

Hay fincas que es que son, pero tremendas

Pero así cualquiera puede poner una cámara. Yo ahora mismo voy a la calle barquillo, compro una cámara por muy poco dinero y la pongo donde sea

En mi casa se lo están planteando

En un balcón y filmo, y yo, que yo sepa no es ilegal

No, hasta ahora no

Será a legal como mucho

Claro

Por eso pienso que debería estar reglamentado, si yo cojo esa cámara y la utilizo y la enfoco al balcón de enfrente y la estoy filmando todo el día

Hombre, yo que se, pero tampoco te vas a poner e esa mala fe.

De todas formas habrá que autorizar el uso de, y habrá que regularlo

Claro, hombre claro, tendrán que ser específicas

Pero depende de que es lo que quieren , porque ayer no se si fue o antes de ayer salió en televisión de Google que puedes entrar y te va acercando, te va acercando y ves en ese momento lo que esté pasando. Pones la dirección

No es a tiempo real

No, pero bueno, me da igual

Se que debe haber cada cosa

No y ha salido una noticia de algo de esto de unas terrazas

Si de una señora que la pillaron haciendo top less

O con el marido de otra o algo así

(risas)

Estaba en la terraza, había subido a la terraza

Cualquiera puede entrar a la página y acercarse, pones la direción, no se como es y se va acercando, se va acercando.

Lo ves como al final estamos más vigilados de lo que creemos

Por eso te digo

No si tenemos, esas son las cámaras que no vemos, las ocho mil que hay

Las ocho mil que hay en satélites

Exacto

Bueno, pues por mi parte daros las gracias. Si queréis añadir algo, alguna sugerencia

Que es muy complicado

Que las sociedades se han vuelto muy vulnerables al terrorismo

Si, si

Hay temor, hay miedo. La delincuencia avanza y hay miedo. Entonces todo el mundo quiere seguridad, pero no a costa de perder la privacidad. Hay que lograr un equilibrio entre seguridad y privacidad

(Hablan a la vez)

Después de los atentados en el metro la gente iba mirando, mirado bolsas, había quién no entraba y había temor

Si, y en EEUU dicen que, eso es lo que dijeron el otro día, que en el próximo atentado los americanos se van a olvidar del 11-S, como va ser el próximo, está ya todo el mundo que no veas, un susto que pa que

Bueno, pues muchas gracias.

ANNEX IV

country = ES

1) Frequency Tables

q1sex[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	male	14	42,4	42,4	42,4
	female	19	57,6	57,6	100,0
	Total	33	100,0	100,0	

a. country = ES

q2age[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18	3	9,1	9,1	9,1
	19	3	9,1	9,1	18,2
	24	2	6,1	6,1	24,2
	27	1	3,0	3,0	27,3
	30	1	3,0	3,0	30,3
	32	1	3,0	3,0	33,3
	36	1	3,0	3,0	36,4
	37	1	3,0	3,0	39,4
	40	1	3,0	3,0	42,4
	42	2	6,1	6,1	48,5
	43	1	3,0	3,0	51,5
	44	2	6,1	6,1	57,6
	46	2	6,1	6,1	63,6
	49	1	3,0	3,0	66,7
	51	1	3,0	3,0	69,7
	54	1	3,0	3,0	72,7
	55	3	9,1	9,1	81,8
	58	1	3,0	3,0	84,8
	61	2	6,1	6,1	90,9
	62	1	3,0	3,0	93,9
	64	1	3,0	3,0	97,0
	69	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q3household Persons in houshold ink self[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	4	12,1	12,1	12,1
	2	8	24,2	24,2	36,4
	3	8	24,2	24,2	60,6
	4 or more	13	39,4	39,4	100,0
	Total	33	100,0	100,0	

a. country = ES

q4children[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	16	48,5	48,5	48,5
	no	17	51,5	51,5	100,0
	Total	33	100,0	100,0	

a. country = ES

q5childhome1 No children[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	14	42,4	42,4	42,4
	yes	19	57,6	57,6	100,0
	Total	33	100,0	100,0	

a. country = ES

q5childhome2 14 or younger[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	78,8	78,8	78,8
	yes	7	21,2	21,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q5childhome3 15 or older[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	25	75,8	75,8	75,8
	yes	8	24,2	24,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q6edu[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	11	33,3	33,3	33,3
	3	1	3,0	3,0	36,4
	4	11	33,3	33,3	69,7
	6	2	6,1	6,1	75,8
	7	8	24,2	24,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q7occupstring[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Actor	1	3,0	3,0	3,0
	Administrative employee	5	15,2	15,2	18,2
	Bank employee	1	3,0	3,0	21,2
	Electric Technician	1	3,0	3,0	24,2
	Employee in Communication Firm	1	3,0	3,0	27,3
	hotel employee	1	3,0	3,0	30,3
	Housewife	6	18,2	18,2	48,5
	Image technician	1	3,0	3,0	51,5
	Informatician	1	3,0	3,0	54,5
	journalist	1	3,0	3,0	57,6
	Manual worker	1	3,0	3,0	60,6
	Office worker	2	6,1	6,1	66,7
	Self-employed	1	3,0	3,0	69,7
	student	3	9,1	9,1	78,8
	Student	4	12,1	12,1	90,9
	teacher	1	3,0	3,0	93,9
	Technician	1	3,0	3,0	97,0
	Unemployed	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q8district[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Metro	27	81,8	81,8	81,8
	Provincial town	5	15,2	15,2	97,0
	Rural	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q9phone[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	30	90,9	90,9	90,9
	at least once a week	2	6,1	6,1	97,0
	never	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q10email[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	10	30,3	30,3	30,3
	at least once a week	9	27,3	27,3	57,6
	at least once a month	2	6,1	6,1	63,6
	less than once a month	2	6,1	6,1	69,7
	never	10	30,3	30,3	100,0
	Total	33	100,0	100,0	

a. country = ES

q11internet[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	16	48,5	48,5	48,5
	at least once a week	7	21,2	21,2	69,7
	at least once a month	1	3,0	3,0	72,7
	less than once a month	1	3,0	3,0	75,8
	never	8	24,2	24,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q12publictransport[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	21	63,6	63,6	63,6
	at least once a week	6	18,2	18,2	81,8
	at least once a month	4	12,1	12,1	93,9
	less than once a month	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q13plane[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	more than 5 times a year	1	3,0	3,0	3,0
	3-5 times a year	3	9,1	9,1	12,1
	1-2 times a year	9	27,3	27,3	39,4
	less than 1 time a year	13	39,4	39,4	78,8
	never	7	21,2	21,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q14car[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	10	30,3	30,3	30,3
	at least once a week	16	48,5	48,5	78,8
	at least once a month	3	9,1	9,1	87,9
	less than once a month	3	9,1	9,1	97,0
	never	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q15general The security of society is absolutely dependent on the development and use of new security technologies[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	6	18,2	18,2	18,2
	partly agree	15	45,5	45,5	63,6
	neither agree nor disagree	6	18,2	18,2	81,8
	partly disagree	5	15,2	15,2	97,0
	completely disagree	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	8	24,2	24,2	24,2
	partly agree	15	45,5	45,5	69,7
	neither agree nor disagree	3	9,1	9,1	78,8
	partly disagree	4	12,1	12,1	90,9
	completely disagree	3	9,1	9,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	9	27,3	27,3	27,3
	partly agree	11	33,3	33,3	60,6
	neither agree nor disagree	1	3,0	3,0	63,6
	partly disagree	7	21,2	21,2	84,8
	completely disagree	5	15,2	15,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q18general When security technology is available, we might just as well make use of it[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	13	39,4	39,4	39,4
	partly agree	11	33,3	33,3	72,7
	neither agree nor disagree	4	12,1	12,1	84,8
	partly disagree	4	12,1	12,1	97,0
	completely disagree	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q19general Privacy should not be violated without reasonable suspicion of criminal intent[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	22	66,7	66,7	66,7
	partly agree	9	27,3	27,3	93,9
	neither agree nor disagree	1	3,0	3,0	97,0
	completely disagree	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	21	63,6	63,6	63,6
	partly agree	10	30,3	30,3	93,9
	completely disagree	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q21general New security technologies are likely to be abused by governmental agencies[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	15	45,5	45,5	45,5
	partly agree	9	27,3	27,3	72,7
	neither agree nor disagree	4	12,1	12,1	84,8
	partly disagree	1	3,0	3,0	87,9
	completely disagree	4	12,1	12,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q22general New security technologies are likely to be abused by criminals[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	17	51,5	51,5	51,5
	partly agree	9	27,3	27,3	78,8
	neither agree nor disagree	4	12,1	12,1	90,9
	partly disagree	2	6,1	6,1	97,0
	completely disagree	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q23biom1 Facial characteristics[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	31	93,9	93,9	93,9
	yes	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q23biom2 Fingerprints[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	15	45,5	45,5	45,5
	yes	18	54,5	54,5	100,0
	Total	33	100,0	100,0	

a. country = ES

q23biom3 Iris recognition[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	23	69,7	69,7	69,7
	yes	10	30,3	30,3	100,0
	Total	33	100,0	100,0	

a. country = ES

q23biom4 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	28	84,8	84,8	84,8
	yes	5	15,2	15,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q23biom5 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	29	87,9	87,9	87,9
	yes	4	12,1	12,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q24biom1 Bank[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	20	60,6	60,6	60,6
	yes	13	39,4	39,4	100,0
	Total	33	100,0	100,0	

a. country = ES

q24biom2 Airport[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	7	21,2	21,2	21,2
	yes	26	78,8	78,8	100,0
	Total	33	100,0	100,0	

a. country = ES

q24biom3 Store[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	30	90,9	90,9	90,9
	yes	3	9,1	9,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q24biom4 Border[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	11	33,3	33,3	33,3
	yes	22	66,7	66,7	100,0
	Total	33	100,0	100,0	

a. country = ES

q24biom5 Central bus and train station[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	20	60,6	60,6	60,6
	yes	13	39,4	39,4	100,0
	Total	33	100,0	100,0	

a. country = ES

q24biom6 Stadium and crowded[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	19	57,6	57,6	57,6
	yes	14	42,4	42,4	100,0
	Total	33	100,0	100,0	

a. country = ES

q24biom7 Other private service[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	30	90,9	90,9	90,9
	yes	3	9,1	9,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q24biom8 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	31	93,9	93,9	93,9
	yes	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q24biom9 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	33	100,0	100,0	100,0

a. country = ES

q25biom Storing biometric data (e.g. fingerprints or DNA samples) of all citizens in a central database is an acceptable step to fight crime[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	5	15,2	15,2	15,2
	partly agree	14	42,4	42,4	57,6
	neither agree nor disagree	5	15,2	15,2	72,7
	partly disagree	7	21,2	21,2	93,9
	completely disagree	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q26biom The use of the biometric passport makes me feel insecure because of the risk of my biometric data being stolen[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	11	33,3	33,3	33,3
	partly agree	14	42,4	42,4	75,8
	neither agree nor disagree	3	9,1	9,1	84,8
	partly disagree	3	9,1	9,1	93,9
	completely disagree	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q27visual1 Store[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	63,6	63,6	63,6
	yes	12	36,4	36,4	100,0
	Total	33	100,0	100,0	

a. country = ES

q27visual2 Dressing room[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	33	100,0	100,0	100,0

a. country = ES

q27visual3 Central bus and train station[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	39,4	39,4	39,4
	yes	20	60,6	60,6	100,0
	Total	33	100,0	100,0	

a. country = ES

q27visual4 Bank[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	39,4	39,4	39,4
	yes	20	60,6	60,6	100,0
	Total	33	100,0	100,0	

a. country = ES

q27visual5 Airport[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	6	18,2	18,2	18,2
	yes	27	81,8	81,8	100,0
	Total	33	100,0	100,0	

a. country = ES

q27visual6 Stadium and crowded[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	12	36,4	36,4	36,4
	yes	21	63,6	63,6	100,0
	Total	33	100,0	100,0	

a. country = ES

q27visual7 All public[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	29	87,9	87,9	87,9
	yes	4	12,1	12,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q27visual8 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	32	97,0	97,0	97,0
	yes	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q27visual9 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	31	93,9	93,9	93,9
	yes	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q28visual How do you feel about the number of CCTV cameras in public spaces in general?[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	there should be more	7	21,2	21,9	21,9
	the number is appropriate	13	39,4	40,6	62,5
	there should be less	7	21,2	21,9	84,4
	there should be no	5	15,2	15,6	100,0
	Total	32	97,0	100,0	
Missing	d.k.	1	3,0		
Total		33	100,0		

a. country = ES

q29visual1 School[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	30	90,9	90,9	90,9
	yes	3	9,1	9,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q29visual2 Central bus and train station[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	48,5	48,5	48,5
	yes	17	51,5	51,5	100,0
	Total	33	100,0	100,0	

a. country = ES

q29visual3 Airport[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	5	15,2	15,2	15,2
	yes	28	84,8	84,8	100,0
	Total	33	100,0	100,0	

a. country = ES

q29visual4 Shopping mall[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	28	84,8	84,8	84,8
	yes	5	15,2	15,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q29visual5 Public buildings[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	51,5	51,5	51,5
	yes	16	48,5	48,5	100,0
	Total	33	100,0	100,0	

a. country = ES

q29visual6 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	31	93,9	93,9	93,9
	yes	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q29visual7 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	29	87,9	87,9	87,9
	yes	4	12,1	12,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q30visual1 Reveal everything[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	78,8	78,8	78,8
	yes	7	21,2	21,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q30visual2 Mannequin projection[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	66,7	66,7	66,7
	yes	11	33,3	33,3	100,0
	Total	33	100,0	100,0	

a. country = ES

q30visual3 Body heat, sweat & heart rate[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	30	90,9	90,9	90,9
	yes	3	9,1	9,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q30visual4 Metal[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	39,4	39,4	39,4
	yes	20	60,6	60,6	100,0
	Total	33	100,0	100,0	

a. country = ES

q30visual5 Luggage x-ray[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	14	42,4	42,4	42,4
	yes	19	57,6	57,6	100,0
	Total	33	100,0	100,0	

a. country = ES

q30visual6 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	32	97,0	97,0	97,0
	yes	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q30visual7 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	33	100,0	100,0	100,0

a. country = ES

q31visual CCTV surveillance makes me feel more secure[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	8	24,2	24,2	24,2
	partly agree	15	45,5	45,5	69,7
	neither agree nor disagree	5	15,2	15,2	84,8
	partly disagree	3	9,1	9,1	93,9
	completely disagree	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q32visual CCTV surveillance infringes my privacy[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	9	27,3	27,3	27,3
	partly agree	16	48,5	48,5	75,8
	neither agree nor disagree	5	15,2	15,2	90,9
	partly disagree	1	3,0	3,0	93,9
	completely disagree	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q33visual Scanning of persons for detection of hidden items is an acceptable tool for preventing terror[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	18	54,5	54,5	54,5
	partly agree	10	30,3	30,3	84,8
	partly disagree	1	3,0	3,0	87,9
	completely disagree	4	12,1	12,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q34local1 Terrorists and criminals w court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	9	27,3	27,3	27,3
	yes	24	72,7	72,7	100,0
	Total	33	100,0	100,0	

a. country = ES

q34local2 Any w/o court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	30	90,9	90,9	90,9
	yes	3	9,1	9,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q34local3 Emergency[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	3	9,1	9,1	9,1
	yes	30	90,9	90,9	100,0
	Total	33	100,0	100,0	

a. country = ES

q34local4 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	32	97,0	97,0	97,0
	yes	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q34local5 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	33	100,0	100,0	100,0

a. country = ES

q35local1 Terrorists and criminals w court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	9	27,3	27,3	27,3
	yes	24	72,7	72,7	100,0
	Total	33	100,0	100,0	

a. country = ES

q35local2 Any w/o court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	30	90,9	90,9	90,9
	yes	3	9,1	9,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q35local3 Stolen vehicles[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	8	24,2	24,2	24,2
	yes	25	75,8	75,8	100,0
	Total	33	100,0	100,0	

a. country = ES

q35local4 Speeding[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	66,7	66,7	66,7
	yes	11	33,3	33,3	100,0
	Total	33	100,0	100,0	

a. country = ES

q35local5 Automatic accident reporting[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	3	9,1	9,1	9,1
	yes	30	90,9	90,9	100,0
	Total	33	100,0	100,0	

a. country = ES

q35local6 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	33	100,0	100,0	100,0

a. country = ES

q35local7 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	33	100,0	100,0	100,0

a. country = ES

q36local Should eCall automatically be installed in all new cars?[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	6	18,2	20,0	20,0
	yes but possible to deactivate	12	36,4	40,0	60,0
	no, optional	12	36,4	40,0	100,0
	Total	30	90,9	100,0	
Missing	d.k.	3	9,1		
Total		33	100,0		

a. country = ES

q37local The possibility of locating all mobile phones is privacy infringing[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	16	48,5	48,5	48,5
	partly agree	10	30,3	30,3	78,8
	neither agree nor disagree	2	6,1	6,1	84,8
	partly disagree	2	6,1	6,1	90,9
	completely disagree	3	9,1	9,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q38local The possibility of locating a suspect's mobile phones is a good tool for the police in investigating and preventing terror and crime[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	18	54,5	54,5	54,5
	partly agree	9	27,3	27,3	81,8
	neither agree nor disagree	3	9,1	9,1	90,9
	partly disagree	2	6,1	6,1	97,0
	completely disagree	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q39local The possibility of locating all cars is privacy infringing[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	15	45,5	45,5	45,5
	partly agree	11	33,3	33,3	78,8
	neither agree nor disagree	3	9,1	9,1	87,9
	partly disagree	2	6,1	6,1	93,9
	completely disagree	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

40local The possibility of locating all cars is a good tool for the police in investigatin and preventing terror and crime[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	11	33,3	33,3	33,3
	partly agree	10	30,3	30,3	63,6
	neither agree nor disagree	7	21,2	21,2	84,8
	partly disagree	2	6,1	6,1	90,9
	completely disagree	3	9,1	9,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q41data1 Prevention of terrorism[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	9	27,3	27,3	27,3
	yes	24	72,7	72,7	100,0
	Total	33	100,0	100,0	

a. country = ES

q41data2 Investigation of terrorism[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	51,5	51,5	51,5
	yes	16	48,5	48,5	100,0
	Total	33	100,0	100,0	

a. country = ES

q41data3 Prevention of crime[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	18	54,5	54,5	54,5
	yes	15	45,5	45,5	100,0
	Total	33	100,0	100,0	

a. country = ES

q41data4 Investigation of crime[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	19	57,6	57,6	57,6
	yes	14	42,4	42,4	100,0
	Total	33	100,0	100,0	

a. country = ES

q41data5 Commercial[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	33	100,0	100,0	100,0

a. country = ES

q41data6 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	32	97,0	97,0	97,0
	yes	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q41data7 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	30	90,9	90,9	90,9
	yes	3	9,1	9,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q42data1 Prevention of terrorism[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	11	33,3	33,3	33,3
	yes	22	66,7	66,7	100,0
	Total	33	100,0	100,0	

a. country = ES

q42data2 Investigation of terrorism[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	51,5	51,5	51,5
	yes	16	48,5	48,5	100,0
	Total	33	100,0	100,0	

a. country = ES

q42data3 Prevention of crime[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	51,5	51,5	51,5
	yes	16	48,5	48,5	100,0
	Total	33	100,0	100,0	

a. country = ES

q42data4 Investigation of crime[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	15	45,5	45,5	45,5
	yes	18	54,5	54,5	100,0
	Total	33	100,0	100,0	

a. country = ES

q42data5 Commercial[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	33	100,0	100,0	100,0

a. country = ES

q42data6 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	33	100,0	100,0	100,0

a. country = ES

q42data7 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	31	93,9	93,9	93,9
	yes	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	9	27,3	27,3	27,3
	partly agree	9	27,3	27,3	54,5
	neither agree nor disagree	3	9,1	9,1	63,6
	partly disagree	10	30,3	30,3	93,9
	completely disagree	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	15	45,5	45,5	45,5
	partly agree	9	27,3	27,3	72,7
	neither agree nor disagree	5	15,2	15,2	87,9
	partly disagree	3	9,1	9,1	97,0
	completely disagree	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q45data Scanning of and combining data from different databases containing personal information is privacy infringing[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	17	51,5	51,5	51,5
	partly agree	8	24,2	24,2	75,8
	neither agree nor disagree	4	12,1	12,1	87,9
	partly disagree	3	9,1	9,1	97,0
	completely disagree	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q46data Scanning of and combining data from different databases is a good tool for police to prevent terror[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	12	36,4	36,4	36,4
	partly agree	9	27,3	27,3	63,6
	neither agree nor disagree	5	15,2	15,2	78,8
	partly disagree	6	18,2	18,2	97,0
	completely disagree	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q47data Databases being used for something else than the original purpose is a serious privacy problem[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	1	3,0	3,0	3,0
	completely agree	26	78,8	78,8	81,8
	partly agree	1	3,0	3,0	84,8
	neither agree nor disagree	1	3,0	3,0	87,9
	partly disagree	1	3,0	3,0	90,9
	completely disagree	3	9,1	9,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q48wire1 Prevention and investigation of terrorism w court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	8	24,2	24,2	24,2
	yes	25	75,8	75,8	100,0
	Total	33	100,0	100,0	

a. country = ES

q48wire2 Prevention and investigation of terrorism w/o court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	63,6	63,6	63,6
	yes	12	36,4	36,4	100,0
	Total	33	100,0	100,0	

a. country = ES

q48wire3 Prevention and investigation of crime w court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	7	21,2	21,2	21,2
	yes	26	78,8	78,8	100,0
	Total	33	100,0	100,0	

a. country = ES

q48wire4 Prevention and investigation of crime w/o court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	24	72,7	72,7	72,7
	yes	9	27,3	27,3	100,0
	Total	33	100,0	100,0	

a. country = ES

q48wire5 Commercial[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	33	100,0	100,0	100,0

a. country = ES

q48wire6 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	33	100,0	100,0	100,0

a. country = ES

q48wire7 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	33	100,0	100,0	100,0

a. country = ES

q49wire What methods of eavesdropping is acceptable?[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	all communication lines	3	9,1	9,1	9,1
	persons that suspect is expected to contact	10	30,3	30,3	39,4
	suspects	17	51,5	51,5	90,9
	totally unacceptable	3	9,1	9,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q50wire Eavesdropping is a good tool for police investigation[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	15	45,5	45,5	45,5
	partly agree	10	30,3	30,3	75,8
	neither agree nor disagree	4	12,1	12,1	87,9
	partly disagree	4	12,1	12,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q51wire Eavesdropping is a serious violation of privacy[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	15	45,5	45,5	45,5
	partly agree	15	45,5	45,5	90,9
	neither agree nor disagree	1	3,0	3,0	93,9
	partly disagree	1	3,0	3,0	97,0
	completely disagree	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q52protect1 Anonymous calling cards[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	23	69,7	69,7	69,7
	yes	10	30,3	30,3	100,0
	Total	33	100,0	100,0	

a. country = ES

q52protect2 Encryption programmes[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	18	54,5	54,5	54,5
	yes	15	45,5	45,5	100,0
	Total	33	100,0	100,0	

a. country = ES

q52protect3 Identity management[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	20	60,6	60,6	60,6
	yes	13	39,4	39,4	100,0
	Total	33	100,0	100,0	

a. country = ES

q52protect4 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	29	87,9	87,9	87,9
	yes	4	12,1	12,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q52protect5 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	78,8	78,8	78,8
	yes	7	21,2	21,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	17	51,5	51,5	51,5
	partly agree	6	18,2	18,2	69,7
	neither agree nor disagree	8	24,2	24,2	93,9
	partly disagree	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q54protect Privacy enhancing technologies should not be legal if they make police investigation and prevention of terror and crime more difficult[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	9	27,3	27,3	27,3
	partly agree	9	27,3	27,3	54,5
	neither agree nor disagree	6	18,2	18,2	72,7
	partly disagree	6	18,2	18,2	90,9
	completely disagree	3	9,1	9,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q55dilem1 Accept registration of travel and fingerprints[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	78,8	78,8	78,8
	yes	7	21,2	21,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q55dilem2 Accept only if template[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	31	93,9	93,9	93,9
	yes	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q55dilem3 Accept only if deleted[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	27	81,8	81,8	81,8
	yes	6	18,2	18,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q55dilem4 Accept only if not exclusive[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	66,7	66,7	66,7
	yes	11	33,3	33,3	100,0
	Total	33	100,0	100,0	

a. country = ES

q55dilem5 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	66,7	66,7	66,7
	yes	11	33,3	33,3	100,0
	Total	33	100,0	100,0	

a. country = ES

q55dilem6 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	31	93,9	93,9	93,9
	yes	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q56dilem1 Accept database and biometrics[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	19	57,6	57,6	57,6
	yes	14	42,4	42,4	100,0
	Total	33	100,0	100,0	

a. country = ES

q56dilem2 Accept naked machine[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	31	93,9	93,9	93,9
	yes	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q56dilem3 Accept sweat, body heat and heart rate scanning[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	29	87,9	87,9	87,9
	yes	4	12,1	12,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q56dilem4 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	24	72,7	72,7	72,7
	yes	9	27,3	27,3	100,0
	Total	33	100,0	100,0	

a. country = ES

q56dilem5 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	25	75,8	75,8	75,8
	yes	8	24,2	24,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q57dilem1 Accept all consequences[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	28	84,8	84,8	84,8
	yes	5	15,2	15,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q57dilem2 Accept only low rate of false positives[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	28	84,8	84,8	84,8
	yes	5	15,2	15,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q57dilem3 Accept only no false positives[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	63,6	63,6	63,6
	yes	12	36,4	36,4	100,0
	Total	33	100,0	100,0	

a. country = ES

q57dilem4 Accept only in exposed places[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	18	54,5	54,5	54,5
	yes	15	45,5	45,5	100,0
	Total	33	100,0	100,0	

a. country = ES

q57dilem5 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	31	93,9	93,9	93,9
	yes	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q57dilem6 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	32	97,0	97,0	97,0
	yes	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q58dilem1 Accept all access for counter terrorism[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	66,7	66,7	66,7
	yes	11	33,3	33,3	100,0
	Total	33	100,0	100,0	

a. country = ES

q58dilem2 Accept only if anonymous and w court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	14	42,4	42,4	42,4
	yes	19	57,6	57,6	100,0
	Total	33	100,0	100,0	

a. country = ES

q58dilem3 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	30	90,9	90,9	90,9
	yes	3	9,1	9,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q58dilem4 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	32	97,0	97,0	97,0
	yes	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q59dilem1 Accept locate car to prevent crime or terrorism[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	11	33,3	33,3	33,3
	yes	22	66,7	66,7	100,0
	Total	33	100,0	100,0	

a. country = ES

q59dilem2 Accept speeding tickets[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	32	97,0	97,0	97,0
	yes	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q59dilem3 Accept register all movements[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	32	97,0	97,0	97,0
	yes	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q59dilem4 Accept only accidents[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	23	69,7	69,7	69,7
	yes	10	30,3	30,3	100,0
	Total	33	100,0	100,0	

a. country = ES

q59dilem5 Accept only if voluntary[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	18	54,5	54,5	54,5
	yes	15	45,5	45,5	100,0
	Total	33	100,0	100,0	

a. country = ES

q59dilem6 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	33	100,0	100,0	100,0

a. country = ES

q60dilem1 Accept calling cards[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	63,6	63,6	63,6
	yes	12	36,4	36,4	100,0
	Total	33	100,0	100,0	

a. country = ES

q60dilem2 Accept encryption[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	66,7	66,7	66,7
	yes	11	33,3	33,3	100,0
	Total	33	100,0	100,0	

a. country = ES

q60dilem3 Accept Internet anonymity - bomb[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	27	81,8	81,8	81,8
	yes	6	18,2	18,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q60dilem4 Accept Internet anonymity - child pornography[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	31	93,9	93,9	93,9
	yes	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q60dilem5 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	63,6	63,6	63,6
	yes	12	36,4	36,4	100,0
	Total	33	100,0	100,0	

a. country = ES

q60dilem6 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	29	87,9	87,9	87,9
	yes	4	12,1	12,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q61dilem1 Accept exclusion of refusers from public service[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	30	90,9	90,9	90,9
	yes	3	9,1	9,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q61dilem2 Accept exclusion of unabled from public service[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	31	93,9	93,9	93,9
	yes	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q61dilem3 Accept refusers are impended when public transport[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	27	81,8	81,8	81,8
	yes	6	18,2	18,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q61dilem4 Accept unabled are impended when public transport[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	29	87,9	87,9	87,9
	yes	4	12,1	12,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q61dilem5 Accept no consequences for refusers[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	63,6	63,6	63,6
	yes	12	36,4	36,4	100,0
	Total	33	100,0	100,0	

a. country = ES

q61dilem6 Accept no consequences for unabled[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	23	69,7	69,7	69,7
	yes	10	30,3	30,3	100,0
	Total	33	100,0	100,0	

a. country = ES

q61dilem7 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	27	81,8	81,8	81,8
	yes	6	18,2	18,2	100,0
	Total	33	100,0	100,0	

a. country = ES

q62demo Politicians must always submit important questions to public debate and public hearings before making decisions on implementing new security technologies[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	23	69,7	69,7	69,7
	partly agree	7	21,2	21,2	90,9
	neither agree nor disagree	2	6,1	6,1	97,0
	partly disagree	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q63demo The subject of security and privacy is so complicated that it makes no sense to include the general public in discussions of this issue[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	3	9,1	9,1	9,1
	partly agree	5	15,2	15,2	24,2
	neither agree nor disagree	6	18,2	18,2	42,4
	partly disagree	8	24,2	24,2	66,7
	completely disagree	11	33,3	33,3	100,0
	Total	33	100,0	100,0	

a. country = ES

q64demo Human rights organisations are always entitled to be heard when important decisions on security and privacy are made[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	25	75,8	75,8	75,8
	partly agree	3	9,1	9,1	84,8
	neither agree nor disagree	3	9,1	9,1	93,9
	partly disagree	2	6,1	6,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q65demo It is important that private companies involved in producing security technologies are also entitled to be heard when important decisions on security and privacy are made[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	16	48,5	48,5	48,5
	partly agree	9	27,3	27,3	75,8
	neither agree nor disagree	4	12,1	12,1	87,9
	partly disagree	3	9,1	9,1	97,0
	completely disagree	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q66demo In relation to significant decisions on the use of security technologies, it is imperative that alternative solutions are elucidated and included in the debate[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	25	75,8	75,8	75,8
	partly agree	5	15,2	15,2	90,9
	neither agree nor disagree	3	9,1	9,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q67suggest Collection of personal data from unsuspicious individuals must be anonymous until identification is authorized by court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	26	78,8	78,8	78,8
	some importance	6	18,2	18,2	97,0
	little importance	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

q68suggest Only authorized personnel can have access to collected personal data[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	30	90,9	90,9	90,9
	some importance	3	9,1	9,1	100,0
	Total	33	100,0	100,0	

a. country = ES

q69suggest Prior to implementing, new security technologies must be checked for privacy impact[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	25	75,8	78,1	78,1
	some importance	7	21,2	21,9	100,0
	Total	32	97,0	100,0	
Missing	d.k.	1	3,0		
Total		33	100,0		

a. country = ES

q70suggest Funding of research projects on new security technologies should be dependent on a thorough analysis of privacy impacts[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	25	75,8	78,1	78,1
	some importance	7	21,2	21,9	100,0
	Total	32	97,0	100,0	
Missing	d.k.	1	3,0		
Total		33	100,0		

a. country = ES

q71end Have you changed your attitude towards security technologies in general in the course of completing this questionnaire?[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes, more positive	5	15,2	16,1	16,1
	yes, more worried	12	36,4	38,7	54,8
	no	14	42,4	45,2	100,0
	Total	31	93,9	100,0	
Missing	d.k.	2	6,1		
Total		33	100,0		

a. country = ES

q72endstring [a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		22	66,7	66,7	66,7
	Analyze risks of all types, especially for the health (x-rays), for commercial purposes and in relation to the violation of private life	1	3,0	3,0	69,7
	As long as these measures are reliable and do not create too much problems for daily life, it is acceptable to violate privacy in this way some criminal act maybe prevented	1	3,0	3,0	72,7
	I believe that we should also think about other types of security such as the one relatef to violence against women	1	3,0	3,0	75,8
	I think it is right to make research on new security technologies but I think these should not focus merely on fighting terrorism because there are many others things that threaten public security. In addition, we should begin to use correctly the tecnolo	1	3,0	3,0	78,8
	I think that all security technology that violate privacy should be optional, that is to say the individual should be free to use . Security should always implemented in order to offer the advantage or the reward to those who use it and disadvantages to	1	3,0	3,0	81,8
	I think that as long as people that have nothing to hide security technologies are very important in our daily life. They bring a lot of more peace. I am in favour of security technologies	1	3,0	3,0	84,8
	I would like to add that it is very difficult that everybody agrees; because something is good for one and bad for other.	1	3,0	3,0	87,9
	In general terms, I disagree with the use of these technologies, because I don´t belive that these technolgies work (It is not possible the control of every criminal act).	1	3,0	3,0	90,9
	The debate suggested is of difficul solution, because (the tecnologies) may invade a right that is intrisic to the person, such as the right to privacy that is an individual right	1	3,0	3,0	93,9
	the issues are too complicated to express an opinion in such a short time, it is necessary to think more and to have more social awareness, there is debate about this. There are some questions that I did not understand whilst some other were actually poin	1	3,0	3,0	97,0
	The knowledge of security technology is crucial, because its implementation in various aspects will produce a a feeling of security and prevention of phenomena like terrorism and criminality	1	3,0	3,0	100,0
	Total	33	100,0	100,0	

a. country = ES

edu3[a]

		Frequency	Percent
Missing	System	33	100,0

a. country = ES

age3[a]

		Frequency	Percent
Missing	System	33	100,0

a. country = ES

eduISCED97[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	lower secondary level of education	11	33,3	33,3	33,3
	upper secondary level of education	12	36,4	36,4	69,7
	first stage of tertiary education	10	30,3	30,3	100,0
	Total	33	100,0	100,0	

a. country = ES

eduISCED97binary Tertiary[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Shorter than tertiary	23	69,7	69,7	69,7
	Tertiary	10	30,3	30,3	100,0
	Total	33	100,0	100,0	

a. country = ES

AgeBinary Age over and under 50[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-49	22	66,7	66,7	66,7
	50+	11	33,3	33,3	100,0
	Total	33	100,0	100,0	

a. country = ES

2) Cross Tabulations - Sex

15general The security of society is absolutely dependent on the development and use of new security technologies * q1sex Crosstabulation[a]

			q1sex		
			male	female	Total
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	2	4	6
		% within q1sex	14,3%	21,1%	18,2%
	partly agree	Count	5	10	15
		% within q1sex	35,7%	52,6%	45,5%
	neither agree nor disagree	Count	4	2	6
		% within q1sex	28,6%	10,5%	18,2%
	partly disagree	Count	3	2	5
		% within q1sex	21,4%	10,5%	15,2%
	completely disagree	Count	0	1	1
		% within q1sex	,0%	5,3%	3,0%
Total		Count	14	19	33
		% within q1sex	100,0%	100,0%	100,0%

a. country = ES

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror * q1sex Crosstabulation[a]

			q1sex		
			male	female	Total
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count	3	5	8
		% within q1sex	21,4%	26,3%	24,2%
	partly agree	Count	7	8	15
		% within q1sex	50,0%	42,1%	45,5%
	neither agree nor disagree	Count	2	1	3
		% within q1sex	14,3%	5,3%	9,1%
	partly disagree	Count	1	3	4
		% within q1sex	7,1%	15,8%	12,1%
	completely disagree	Count	1	2	3
		% within q1sex	7,1%	10,5%	9,1%
Total		Count	14	19	33
		% within q1sex	100,0%	100,0%	100,0%

a. country = ES

l7general If you have nothing to hide you don't have to worry about security technologies that infring your privacy * q1sex Crosstabulation[a]

			q1sex		
			male	female	Total
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	4	5	9
		% within q1sex	28,6%	26,3%	27,3%
	partly agree	Count	3	8	11
		% within q1sex	21,4%	42,1%	33,3%
	neither agree nor disagree	Count	0	1	1
		% within q1sex	,0%	5,3%	3,0%
	partly disagree	Count	5	2	7
		% within q1sex	35,7%	10,5%	21,2%
	completely disagree	Count	2	3	5
		% within q1sex	14,3%	15,8%	15,2%
Total		Count	14	19	33
		% within q1sex	100,0%	100,0%	100,0%

a. country = ES

q18general When security technology is available, we might just as well make use of it * q1sex Crosstabulation[a]

			q1sex		
			male	female	Total
q18general When security technology is available, we might just as well make use of it	completely agree	Count	6	7	13
		% within q1sex	42,9%	36,8%	39,4%
	partly agree	Count	5	6	11
		% within q1sex	35,7%	31,6%	33,3%
	neither agree nor disagree	Count	1	3	4
		% within q1sex	7,1%	15,8%	12,1%
	partly disagree	Count	2	2	4
		% within q1sex	14,3%	10,5%	12,1%
	completely disagree	Count	0	1	1
		% within q1sex	,0%	5,3%	3,0%
Total		Count	14	19	33
		% within q1sex	100,0%	100,0%	100,0%

a. country = ES

q19general Privacy should not be violated without reasonable suspicion of criminal intent * q1sex Crosstabulation[a]

			q1sex		
			male	female	Total
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	9	13	22
		% within q1sex	64,3%	68,4%	66,7%
	partly agree	Count	4	5	9
		% within q1sex	28,6%	26,3%	27,3%
	neither agree nor disagree	Count	1	0	1
		% within q1sex	7,1%	,0%	3,0%
	completely disagree	Count	0	1	1
		% within q1sex	,0%	5,3%	3,0%
Total		Count	14	19	33
		% within q1sex	100,0%	100,0%	100,0%

a. country = ES

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent * q1sex Crosstabulation[a]

			q1sex		
			male	female	Total
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	8	13	21
		% within q1sex	57,1%	68,4%	63,6%
	partly agree	Count	5	5	10
		% within q1sex	35,7%	26,3%	30,3%
	completely disagree	Count	1	1	2
		% within q1sex	7,1%	5,3%	6,1%
Total		Count	14	19	33
		% within q1sex	100,0%	100,0%	100,0%

a. country = ES

q21general New security technologies are likely to be abused by governmental agencies * q1sex Crosstabulation[a]

			q1sex		
			male	female	Total
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	7	8	15
		% within q1sex	50,0%	42,1%	45,5%
	partly agree	Count	6	3	9
		% within q1sex	42,9%	15,8%	27,3%
	neither agree nor disagree	Count	0	4	4
		% within q1sex	,0%	21,1%	12,1%
	partly disagree	Count	1	0	1
		% within q1sex	7,1%	,0%	3,0%
	completely disagree	Count	0	4	4
		% within q1sex	,0%	21,1%	12,1%
Total		Count	14	19	33
		% within q1sex	100,0%	100,0%	100,0%

a. country = ES

q22general New security technologies are likely to be abused by criminals * q1sex Crosstabulation[a]

			q1sex		
			male	female	Total
q22general New security technologies are likely to be abused by criminals	completely agree	Count	10	7	17
		% within q1sex	71,4%	36,8%	51,5%
	partly agree	Count	2	7	9
		% within q1sex	14,3%	36,8%	27,3%
	neither agree nor disagree	Count	2	2	4
		% within q1sex	14,3%	10,5%	12,1%
	partly disagree	Count	0	2	2
		% within q1sex	,0%	10,5%	6,1%
	completely disagree	Count	0	1	1
		% within q1sex	,0%	5,3%	3,0%
Total		Count	14	19	33
		% within q1sex	100,0%	100,0%	100,0%

a. country = ES

3) Cross Tabulations – Age

q15general The security of society is absolutely dependent on the development and use of new security technologies * AgeBinary Age over and under 50 Crosstabulation[a]

			AgeBinary Age over and under 50		
			18-49	50+	Total
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	5	1	6
		% within AgeBinary Age over and under 50	22,7%	9,1%	18,2%
	partly agree	Count	12	3	15
		% within AgeBinary Age over and under 50	54,5%	27,3%	45,5%
	neither agree nor disagree	Count	2	4	6
		% within AgeBinary Age over and under 50	9,1%	36,4%	18,2%
	partly disagree	Count	3	2	5
		% within AgeBinary Age over and under 50	13,6%	18,2%	15,2%
	completely disagree	Count	0	1	1
		% within AgeBinary Age over and under 50	,0%	9,1%	3,0%
Total		Count	22	11	33
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

a. country = ES

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror * AgeBinary Age over and under 50 Crosstabulation[a]

			AgeBinary Age over and under 50		
			18-49	50+	Total
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count	6	2	8
		% within AgeBinary Age over and under 50	27,3%	18,2%	24,2%
	partly agree	Count	11	4	15
		% within AgeBinary Age over and under 50	50,0%	36,4%	45,5%
	neither agree nor disagree	Count	2	1	3
		% within AgeBinary Age over and under 50	9,1%	9,1%	9,1%
	partly disagree	Count	2	2	4
		% within AgeBinary Age over and under 50	9,1%	18,2%	12,1%
	completely disagree	Count	1	2	3
		% within AgeBinary Age over and under 50	4,5%	18,2%	9,1%
Total		Count	22	11	33
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

a. country = ES

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy * AgeBinary Age over and under 50 Crosstabulation[a]

			AgeBinary Age over and under 50		
			18-49	50+	Total
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	6	3	9
		% within AgeBinary Age over and under 50	27,3%	27,3%	27,3%
	partly agree	Count	7	4	11
		% within AgeBinary Age over and under 50	31,8%	36,4%	33,3%
	neither agree nor disagree	Count	0	1	1
		% within AgeBinary Age over and under 50	,0%	9,1%	3,0%
	partly disagree	Count	6	1	7
		% within AgeBinary Age over and under 50	27,3%	9,1%	21,2%
	completely disagree	Count	3	2	5
		% within AgeBinary Age over and under 50	13,6%	18,2%	15,2%
Total		Count	22	11	33
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

a. country = ES

q18general When security technology is available, we might just as well make use of it * AgeBinary Age over and under 50 Crosstabulation[a]

			AgeBinary Age over and under 50		
			18-49	50+	Total
q18general When security technology is available, we might just as well make use of it	completely agree	Count	6	7	13
		% within AgeBinary Age over and under 50	27,3%	63,6%	39,4%
	partly agree	Count	9	2	11
		% within AgeBinary Age over and under 50	40,9%	18,2%	33,3%
	neither agree nor disagree	Count	4	0	4
		% within AgeBinary Age over and under 50	18,2%	,0%	12,1%
	partly disagree	Count	2	2	4
		% within AgeBinary Age over and under 50	9,1%	18,2%	12,1%
	completely disagree	Count	1	0	1
		% within AgeBinary Age over and under 50	4,5%	,0%	3,0%
Total		Count	22	11	33
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

a. country = ES

q19general Privacy should not be violated without reasonable suspicion of criminal intent * AgeBinary Age over and under 50 Crosstabulation[a]

			AgeBinary Age over and under 50		
			18-49	50+	Total
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	16	6	22
		% within AgeBinary Age over and under 50	72,7%	54,5%	66,7%
	partly agree	Count	4	5	9
		% within AgeBinary Age over and under 50	18,2%	45,5%	27,3%
	neither agree nor disagree	Count	1	0	1
		% within AgeBinary Age over and under 50	4,5%	,0%	3,0%
	completely disagree	Count	1	0	1
		% within AgeBinary Age over and under 50	4,5%	,0%	3,0%
Total		Count	22	11	33
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

a. country = ES

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent * AgeBinary Age over and under 50 Crosstabulation[a]

			AgeBinary Age over and under 50		
			18-49	50+	Total
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	16	5	21
		% within AgeBinary Age over and under 50	72,7%	45,5%	63,6%
	partly agree	Count	6	4	10
		% within AgeBinary Age over and under 50	27,3%	36,4%	30,3%
	completely disagree	Count	0	2	2
		% within AgeBinary Age over and under 50	,0%	18,2%	6,1%
Total		Count	22	11	33
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

a. country = ES

q21general New security technologies are likely to be abused by governmental agencies * AgeBinary Age over and under 50 Crosstabulation[a]

			AgeBinary Age over and under 50		
			18-49	50+	Total
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	12	3	15
		% within AgeBinary Age over and under 50	54,5%	27,3%	45,5%
	partly agree	Count	5	4	9
		% within AgeBinary Age over and under 50	22,7%	36,4%	27,3%
	neither agree nor disagree	Count	2	2	4
		% within AgeBinary Age over and under 50	9,1%	18,2%	12,1%
	partly disagree	Count	0	1	1
		% within AgeBinary Age over and under 50	,0%	9,1%	3,0%
	completely disagree	Count	3	1	4
		% within AgeBinary Age over and under 50	13,6%	9,1%	12,1%
Total		Count	22	11	33
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

a. country = ES

q22general New security technologies are likely to be abused by criminals * AgeBinary Age over and under 50 Crosstabulation[a]

			AgeBinary Age over and under 50		
			18-49	50+	Total
q22general New security technologies are likely to be abused by criminals	completely agree	Count	10	7	17
		% within AgeBinary Age over and under 50	45,5%	63,6%	51,5%
	partly agree	Count	6	3	9
		% within AgeBinary Age over and under 50	27,3%	27,3%	27,3%
	neither agree nor disagree	Count	3	1	4
		% within AgeBinary Age over and under 50	13,6%	9,1%	12,1%
	partly disagree	Count	2	0	2
		% within AgeBinary Age over and under 50	9,1%	,0%	6,1%
	completely disagree	Count	1	0	1
		% within AgeBinary Age over and under 50	4,5%	,0%	3,0%
Total		Count	22	11	33
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

a. country = ES

4) Cross Tabulations – Education

q15general The security of society is absolutely dependent on the development and use of new security technologies * eduISCED97binary Tertiary Crosstabulation[a]

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	3	3	6
		% within eduISCED97binary Tertiary	13,0%	30,0%	18,2%
	partly agree	Count	13	2	15
		% within eduISCED97binary Tertiary	56,5%	20,0%	45,5%
	neither agree nor disagree	Count	5	1	6
		% within eduISCED97binary Tertiary	21,7%	10,0%	18,2%
	partly disagree	Count	2	3	5
		% within eduISCED97binary Tertiary	8,7%	30,0%	15,2%
	completely disagree	Count	0	1	1
		% within eduISCED97binary Tertiary	,0%	10,0%	3,0%
Total		Count	23	10	33
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

a. country = ES

16general Many security technologies do not really increase security, but are only being applied to show tha something is done to fight terror * eduISCED97binary Tertiary Crosstabulation[a]

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count	7	1	8
		% within eduISCED97binary Tertiary	30,4%	10,0%	24,2%
	partly agree	Count	11	4	15
		% within eduISCED97binary Tertiary	47,8%	40,0%	45,5%
	neither agree nor disagree	Count	3	0	3
		% within eduISCED97binary Tertiary	13,0%	,0%	9,1%
	partly disagree	Count	1	3	4
		% within eduISCED97binary Tertiary	4,3%	30,0%	12,1%
	completely disagree	Count	1	2	3
		% within eduISCED97binary Tertiary	4,3%	20,0%	9,1%
Total		Count	23	10	33
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

a. country = ES

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy * eduISCED97binary Tertiary Crosstabulation[a]

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	6	3	9
		% within eduISCED97binary Tertiary	26,1%	30,0%	27,3%
	partly agree	Count	8	3	11
		% within eduISCED97binary Tertiary	34,8%	30,0%	33,3%
	neither agree nor disagree	Count	1	0	1
		% within eduISCED97binary Tertiary	4,3%	,0%	3,0%
	partly disagree	Count	5	2	7
		% within eduISCED97binary Tertiary	21,7%	20,0%	21,2%
	completely disagree	Count	3	2	5
		% within eduISCED97binary Tertiary	13,0%	20,0%	15,2%
Total		Count	23	10	33
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

a. country = ES

q18general When security technology is available, we might just as well make use of it * eduISCED97binary Tertiary Crosstabulation[a]

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q18general When security technology is available, we might just as well make use of it	completely agree	Count	10	3	13
		% within eduISCED97binary Tertiary	43,5%	30,0%	39,4%
	partly agree	Count	7	4	11
		% within eduISCED97binary Tertiary	30,4%	40,0%	33,3%
	neither agree nor disagree	Count	3	1	4
		% within eduISCED97binary Tertiary	13,0%	10,0%	12,1%
	partly disagree	Count	2	2	4
		% within eduISCED97binary Tertiary	8,7%	20,0%	12,1%
	completely disagree	Count	1	0	1
		% within eduISCED97binary Tertiary	4,3%	,0%	3,0%
Total		Count	23	10	33
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

a. country = ES

q19general Privacy should not be violated without reasonable suspicion of criminal intent * eduISCED97binary Tertiary Crosstabulation[a]

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	19	3	22
		% within eduISCED97binary Tertiary	82,6%	30,0%	66,7%
	partly agree	Count	3	6	9
		% within eduISCED97binary Tertiary	13,0%	60,0%	27,3%
	neither agree nor disagree	Count	1	0	1
		% within eduISCED97binary Tertiary	4,3%	,0%	3,0%
	completely disagree	Count	0	1	1
		% within eduISCED97binary Tertiary	,0%	10,0%	3,0%
Total		Count	23	10	33
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

a. country = ES

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent * eduISCED97binary Tertiary Crosstabulation[a]

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	15	6	21
		% within eduISCED97binary Tertiary	65,2%	60,0%	63,6%
	partly agree	Count	7	3	10
		% within eduISCED97binary Tertiary	30,4%	30,0%	30,3%
	completely disagree	Count	1	1	2
		% within eduISCED97binary Tertiary	4,3%	10,0%	6,1%
Total		Count	23	10	33
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

a. country = ES

q21general New security technologies are likely to be abused by governmental agencies * eduISCED97binary Tertiary Crosstabulation[a]

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	10	5	15
		% within eduISCED97binary Tertiary	43,5%	50,0%	45,5%
	partly agree	Count	8	1	9
		% within eduISCED97binary Tertiary	34,8%	10,0%	27,3%
	neither agree nor disagree	Count	3	1	4
		% within eduISCED97binary Tertiary	13,0%	10,0%	12,1%
	partly disagree	Count	0	1	1
		% within eduISCED97binary Tertiary	,0%	10,0%	3,0%
	completely disagree	Count	2	2	4
		% within eduISCED97binary Tertiary	8,7%	20,0%	12,1%
Total		Count	23	10	33
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

a. country = ES

q22general New security technologies are likely to be abused by criminals * eduISCED97binary Tertiary Crosstabulation[a]

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q22general New security technologies are likely to be abused by criminals	completely agree	Count	12	5	17
		% within eduISCED97binary Tertiary	52,2%	50,0%	51,5%
	partly agree	Count	6	3	9
		% within eduISCED97binary Tertiary	26,1%	30,0%	27,3%
	neither agree nor disagree	Count	4	0	4
		% within eduISCED97binary Tertiary	17,4%	,0%	12,1%
	partly disagree	Count	1	1	2
		% within eduISCED97binary Tertiary	4,3%	10,0%	6,1%
	completely disagree	Count	0	1	1
		% within eduISCED97binary Tertiary	,0%	10,0%	3,0%
Total		Count	23	10	33
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

a. country = ES

6) Cross Tabulations – Children

q15general The security of society is absolutely dependent on the development and use of new security technologies * q4children Crosstabulation[a]

			q4children		
			yes	no	Total
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	2	4	6
		% within q4children	12,5%	23,5%	18,2%
	partly agree	Count	7	8	15
		% within q4children	43,8%	47,1%	45,5%
	neither agree nor disagree	Count	3	3	6
		% within q4children	18,8%	17,6%	18,2%
	partly disagree	Count	3	2	5
		% within q4children	18,8%	11,8%	15,2%
	completely disagree	Count	1	0	1
		% within q4children	6,3%	,0%	3,0%
Total		Count	16	17	33
		% within q4children	100,0%	100,0%	100,0%

a. country = ES

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror * q4children Crosstabulation[a]

			q4children		
			yes	no	Total
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count	5	3	8
		% within q4children	31,3%	17,6%	24,2%
	partly agree	Count	5	10	15
		% within q4children	31,3%	58,8%	45,5%
	neither agree nor disagree	Count	2	1	3
		% within q4children	12,5%	5,9%	9,1%
	partly disagree	Count	2	2	4
		% within q4children	12,5%	11,8%	12,1%
	completely disagree	Count	2	1	3
		% within q4children	12,5%	5,9%	9,1%
Total		Count	16	17	33
		% within q4children	100,0%	100,0%	100,0%

a. country = ES

7general If you have nothing to hide you don't have to worry about security technologies that infringe you privacy * q4children Crosstabulation[a]

			q4children		
			yes	no	Total
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	2	7	9
		% within q4children	12,5%	41,2%	27,3%
	partly agree	Count	8	3	11
		% within q4children	50,0%	17,6%	33,3%
	neither agree nor disagree	Count	1	0	1
		% within q4children	6,3%	,0%	3,0%
	partly disagree	Count	3	4	7
		% within q4children	18,8%	23,5%	21,2%
	completely disagree	Count	2	3	5
		% within q4children	12,5%	17,6%	15,2%
Total		Count	16	17	33
		% within q4children	100,0%	100,0%	100,0%

a. country = ES

q18general When security technology is available, we might just as well make use of it * q4children Crosstabulation[a]

			q4children		
			yes	no	Total
q18general When security technology is available, we might just as well make use of it	completely agree	Count	8	5	13
		% within q4children	50,0%	29,4%	39,4%
	partly agree	Count	5	6	11
		% within q4children	31,3%	35,3%	33,3%
	neither agree nor disagree	Count	1	3	4
		% within q4children	6,3%	17,6%	12,1%
	partly disagree	Count	2	2	4
		% within q4children	12,5%	11,8%	12,1%
	completely disagree	Count	0	1	1
		% within q4children	,0%	5,9%	3,0%
Total		Count	16	17	33
		% within q4children	100,0%	100,0%	100,0%

a. country = ES

q19general Privacy should not be violated without reasonable suspicion of criminal intent * q4children Crosstabulation[a]

			q4children		
			yes	no	Total
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	11	11	22
		% within q4children	68,8%	64,7%	66,7%
	partly agree	Count	5	4	9
		% within q4children	31,3%	23,5%	27,3%
	neither agree nor disagree	Count	0	1	1
		% within q4children	,0%	5,9%	3,0%
	completely disagree	Count	0	1	1
		% within q4children	,0%	5,9%	3,0%
Total		Count	16	17	33
		% within q4children	100,0%	100,0%	100,0%

a. country = ES

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent * q4children Crosstabulation[a]

			q4children		
			yes	no	Total
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	12	9	21
		% within q4children	75,0%	52,9%	63,6%
	partly agree	Count	3	7	10
		% within q4children	18,8%	41,2%	30,3%
	completely disagree	Count	1	1	2
		% within q4children	6,3%	5,9%	6,1%
Total		Count	16	17	33
		% within q4children	100,0%	100,0%	100,0%

a. country = ES

q21general New security technologies are likely to be abused by governmental agencies * q4children Crosstabulation[a]

			q4children		
			yes	no	Total
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	7	8	15
		% within q4children	43,8%	47,1%	45,5%
	partly agree	Count	3	6	9
		% within q4children	18,8%	35,3%	27,3%
	neither agree nor disagree	Count	3	1	4
		% within q4children	18,8%	5,9%	12,1%
	partly disagree	Count	0	1	1
		% within q4children	,0%	5,9%	3,0%
	completely disagree	Count	3	1	4
		% within q4children	18,8%	5,9%	12,1%
Total		Count	16	17	33
		% within q4children	100,0%	100,0%	100,0%

a. country = ES

q22general New security technologies are likely to be abused by criminals * q4children Crosstabulation[a]

			q4children		
			yes	no	Total
q22general New security technologies are likely to be abused by criminals	completely agree	Count	7	10	17
		% within q4children	43,8%	58,8%	51,5%
	partly agree	Count	5	4	9
		% within q4children	31,3%	23,5%	27,3%
	neither agree nor disagree	Count	2	2	4
		% within q4children	12,5%	11,8%	12,1%
	partly disagree	Count	1	1	2
		% within q4children	6,3%	5,9%	6,1%
	completely disagree	Count	1	0	1
		% within q4children	6,3%	,0%	3,0%
Total		Count	16	17	33
		% within q4children	100,0%	100,0%	100,0%

a. country = ES

q15general The security of society is absolutely dependent on the development and use of new security technologies * q5childhome1 No children Crosstabulation[a]

			q5childhome1 No children		
			no	yes	Total
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	3	3	6
		% within q5childhome1 No children	21,4%	15,8%	18,2%
	partly agree	Count	6	9	15
		% within q5childhome1 No children	42,9%	47,4%	45,5%
	neither agree nor disagree	Count	2	4	6
		% within q5childhome1 No children	14,3%	21,1%	18,2%
	partly disagree	Count	3	2	5
		% within q5childhome1 No children	21,4%	10,5%	15,2%
	completely disagree	Count	0	1	1
		% within q5childhome1 No children	,0%	5,3%	3,0%
Total		Count	14	19	33
		% within q5childhome1 No children	100,0%	100,0%	100,0%

a. country = ES

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror * q5childhome1 No children Crosstabulation[a]

			q5childhome1 No children		
			no	yes	Total
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count	4	4	8
		% within q5childhome1 No children	28,6%	21,1%	24,2%
	partly agree	Count	4	11	15
		% within q5childhome1 No children	28,6%	57,9%	45,5%
	neither agree nor disagree	Count	3	0	3
		% within q5childhome1 No children	21,4%	,0%	9,1%
	partly disagree	Count	2	2	4
		% within q5childhome1 No children	14,3%	10,5%	12,1%
	completely disagree	Count	1	2	3
		% within q5childhome1 No children	7,1%	10,5%	9,1%
Total		Count	14	19	33
		% within q5childhome1 No children	100,0%	100,0%	100,0%

a. country = ES

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy * q5childhome1 No children Crosstabulation[a]

			q5childhome1 No children		
			no	yes	Total
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	2	7	9
		% within q5childhome1 No children	14,3%	36,8%	27,3%
	partly agree	Count	7	4	11
		% within q5childhome1 No children	50,0%	21,1%	33,3%
	neither agree nor disagree	Count	1	0	1
		% within q5childhome1 No children	7,1%	,0%	3,0%
	partly disagree	Count	3	4	7
		% within q5childhome1 No children	21,4%	21,1%	21,2%
	completely disagree	Count	1	4	5
		% within q5childhome1 No children	7,1%	21,1%	15,2%
Total		Count	14	19	33
		% within q5childhome1 No children	100,0%	100,0%	100,0%

a. country = ES

18general When security technology is available, we might just as well make use of it * q5childhome1 No children Crosstabulation[a]

			q5childhome1 No children		
			no	yes	Total
q18general When security technology is available, we might just as well make use of it	completely agree	Count	6	7	13
		% within q5childhome1 No children	42,9%	36,8%	39,4%
	partly agree	Count	5	6	11
		% within q5childhome1 No children	35,7%	31,6%	33,3%
	neither agree nor disagree	Count	2	2	4
		% within q5childhome1 No children	14,3%	10,5%	12,1%
	partly disagree	Count	1	3	4
		% within q5childhome1 No children	7,1%	15,8%	12,1%
	completely disagree	Count	0	1	1
		% within q5childhome1 No children	,0%	5,3%	3,0%
Total		Count	14	19	33
		% within q5childhome1 No children	100,0%	100,0%	100,0%

a. country = ES

19general Privacy should not be violated without reasonable suspicion of criminal intent * q5childhome1 No children Crosstabulation[a]

			q5childhome1 No children		
			no	yes	Total
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	10	12	22
		% within q5childhome1 No children	71,4%	63,2%	66,7%
	partly agree	Count	3	6	9
		% within q5childhome1 No children	21,4%	31,6%	27,3%
	neither agree nor disagree	Count	1	0	1
		% within q5childhome1 No children	7,1%	,0%	3,0%
	completely disagree	Count	0	1	1
		% within q5childhome1 No children	,0%	5,3%	3,0%
Total		Count	14	19	33
		% within q5childhome1 No children	100,0%	100,0%	100,0%

a. country = ES

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent * q5childhome1 No children Crosstabulation[a]

			q5childhome1 No children		
			no	yes	Total
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	10	11	21
		% within q5childhome1 No children	71,4%	57,9%	63,6%
	partly agree	Count	3	7	10
		% within q5childhome1 No children	21,4%	36,8%	30,3%
	completely disagree	Count	1	1	2
		% within q5childhome1 No children	7,1%	5,3%	6,1%
Total		Count	14	19	33
		% within q5childhome1 No children	100,0%	100,0%	100,0%

a. country = ES

q21general New security technologies are likely to be abused by governmental agencies * q5childhome1 No children Crosstabulation[a]

			q5childhome1 No children		
			no	yes	Total
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	6	9	15
		% within q5childhome1 No children	42,9%	47,4%	45,5%
	partly agree	Count	3	6	9
		% within q5childhome1 No children	21,4%	31,6%	27,3%
	neither agree nor disagree	Count	2	2	4
		% within q5childhome1 No children	14,3%	10,5%	12,1%
	partly disagree	Count	0	1	1
		% within q5childhome1 No children	,0%	5,3%	3,0%
	completely disagree	Count	3	1	4
		% within q5childhome1 No children	21,4%	5,3%	12,1%
Total		Count	14	19	33
		% within q5childhome1 No children	100,0%	100,0%	100,0%

a. country = ES

q22general New security technologies are likely to be abused by criminals * q5childhome1 No children Crosstabulation[a]

			q5childhome1 No children		
			no	yes	Total
q22general New security technologies are likely to be abused by criminals	completely agree	Count	6	11	17
		% within q5childhome1 No children	42,9%	57,9%	51,5%
	partly agree	Count	4	5	9
		% within q5childhome1 No children	28,6%	26,3%	27,3%
	neither agree nor disagree	Count	2	2	4
		% within q5childhome1 No children	14,3%	10,5%	12,1%
	partly disagree	Count	1	1	2
		% within q5childhome1 No children	7,1%	5,3%	6,1%
	completely disagree	Count	1	0	1
		% within q5childhome1 No children	7,1%	,0%	3,0%
Total		Count	14	19	33
		% within q5childhome1 No children	100,0%	100,0%	100,0%

a. country = ES

7) Crosstabulations – Transports (plane)

q24biom2 Airport * PlaneBinary Plane more than once a year / less Crosstabulation[a]

			PlaneBinary Plane more than once a year / less		
			1-2 times a year or more	Less than 1 time a year	Total
q24biom2 Airport	no	Count	5	2	7
		% within PlaneBinary Plane more than once a year / less	38,5%	10,0%	21,2%
	yes	Count	8	18	26
		% within PlaneBinary Plane more than once a year / less	61,5%	90,0%	78,8%
Total		Count	13	20	33
		% within PlaneBinary Plane more than once a year / less	100,0%	100,0%	100,0%

a. country = ES

q56dilem1 Accept database and biometrics * PlaneBinary Plane more than once a year / less Crosstabulation[a]

			PlaneBinary Plane more than once a year / less		
			1-2 times a year or more	Less than 1 time a year	Total
q56dilem1 Accept database and biometrics	no	Count	5	14	19
		% within PlaneBinary Plane more than once a year / less	38,5%	70,0%	57,6%
	yes	Count	8	6	14
		% within PlaneBinary Plane more than once a year / less	61,5%	30,0%	42,4%
Total		Count	13	20	33
		% within PlaneBinary Plane more than once a year / less	100,0%	100,0%	100,0%

a. country = ES

8) Crosstabulations – Public Transports

q24biom5 Central bus and train station * PublicBinary Public daily / less Crosstabulation[a]

			PublicBinary Public daily / less		
			Less	Daily	Total
q24biom5 Central bus and train station	no	Count	8	12	20
		% within PublicBinary Public daily / less	66,7%	57,1%	60,6%
	yes	Count	4	9	13
		% within PublicBinary Public daily / less	33,3%	42,9%	39,4%
Total		Count	12	21	33
		% within PublicBinary Public daily / less	100,0%	100,0%	100,0%

a. country = ES

q55dilem1 Accept registration of travel and fingerprints * PublicBinary Public daily / less Crosstabulation[a]

			PublicBinary Public daily / less		
			Less	Daily	Total
q55dilem1 Accept registration of travel and fingerprints	no	Count	10	16	26
		% within PublicBinary Public daily / less	83,3%	76,2%	78,8%
	yes	Count	2	5	7
		% within PublicBinary Public daily / less	16,7%	23,8%	21,2%
Total		Count	12	21	33
		% within PublicBinary Public daily / less	100,0%	100,0%	100,0%

a. country = ES

9) Crosstabulations – Transports (car)

q35local1 Terrorists and criminals w court order * CarBinary Car daily / less Crosstabulation[a]

			CarBinary Car daily / less		
			Less	Daily	Total
q35local1 Terrorists and criminals w court order	no	Count	8	1	9
		% within CarBinary Car daily / less	34,8%	10,0%	27,3%
	yes	Count	15	9	24
		% within CarBinary Car daily / less	65,2%	90,0%	72,7%
Total		Count	23	10	33
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = ES

q35local2 Any w/o court order * CarBinary Car daily / less Crosstabulation[a]

			CarBinary Car daily / less		
			Less	Daily	Total
q35local2 Any w/o court order	no	Count	21	9	30
		% within CarBinary Car daily / less	91,3%	90,0%	90,9%
	yes	Count	2	1	3
		% within CarBinary Car daily / less	8,7%	10,0%	9,1%
Total		Count	23	10	33
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = ES

q35local3 Stolen vehicles * CarBinary Car daily / less Crosstabulation[a]

			CarBinary Car daily / less		
			Less	Daily	Total
q35local3 Stolen vehicles	no	Count	6	2	8
		% within CarBinary Car daily / less	26,1%	20,0%	24,2%
	yes	Count	17	8	25
		% within CarBinary Car daily / less	73,9%	80,0%	75,8%
Total		Count	23	10	33
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = ES

q35local4 Speeding * CarBinary Car daily / less Crosstabulation[a]

			CarBinary Car daily / less		
			Less	Daily	Total
q35local4 Speeding	no	Count	15	7	22
		% within CarBinary Car daily / less	65,2%	70,0%	66,7%
	yes	Count	8	3	11
		% within CarBinary Car daily / less	34,8%	30,0%	33,3%
Total		Count	23	10	33
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = ES

q35local5 Automatic accident reporting * CarBinary Car daily / less Crosstabulation[a]

			CarBinary Car daily / less		
			Less	Daily	Total
q35local5 Automatic accident reporting	no	Count	1	2	3
		% within CarBinary Car daily / less	4,3%	20,0%	9,1%
	yes	Count	22	8	30
		% within CarBinary Car daily / less	95,7%	80,0%	90,9%
Total		Count	23	10	33
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = ES

q36local Should eCall automatically be installed in all new cars? * CarBinary Car daily / less Crosstabulation[a]

			CarBinary Car daily / less		
			Less	Daily	Total
q36local Should eCall automatically be installed in all new cars?	yes	Count	4	2	6
		% within CarBinary Car daily / less	20,0%	20,0%	20,0%
	yes but possible to deactivate	Count	7	5	12
		% within CarBinary Car daily / less	35,0%	50,0%	40,0%
	no, optional	Count	9	3	12
		% within CarBinary Car daily / less	45,0%	30,0%	40,0%
Total		Count	20	10	30
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = ES

q39local The possibility of locating all cars is privacy infringing * CarBinary Car daily / less Crosstabulation[a]

			CarBinary Car daily / less		
			Less	Daily	Total
q39local The possibility of locating all cars is privacy infringing	completely agree	Count	10	5	15
		% within CarBinary Car daily / less	43,5%	50,0%	45,5%
	partly agree	Count	8	3	11
		% within CarBinary Car daily / less	34,8%	30,0%	33,3%
	neither agree nor disagree	Count	2	1	3
		% within CarBinary Car daily / less	8,7%	10,0%	9,1%
	partly disagree	Count	1	1	2
		% within CarBinary Car daily / less	4,3%	10,0%	6,1%
	completely disagree	Count	2	0	2
		% within CarBinary Car daily / less	8,7%	,0%	6,1%
Total		Count	23	10	33
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = ES

q59dilem1 Accept locate car to prevent crime or terrorism * CarBinary Car daily / less Crosstabulation[a]

			CarBinary Car daily / less		
			Less	Daily	Total
q59dilem1 Accept locate car to prevent crime or terrorism	no	Count	8	3	11
		% within CarBinary Car daily / less	34,8%	30,0%	33,3%
	yes	Count	15	7	22
		% within CarBinary Car daily / less	65,2%	70,0%	66,7%
Total		Count	23	10	33
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = ES

q59dilem2 Accept speeding tickets * CarBinary Car daily / less Crosstabulation[a]

			CarBinary Car daily / less		
			Less	Daily	Total
q59dilem2 Accept speeding tickets	no	Count	22	10	32
		% within CarBinary Car daily / less	95,7%	100,0%	97,0%
	yes	Count	1	0	1
		% within CarBinary Car daily / less	4,3%	,0%	3,0%
Total		Count	23	10	33
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = ES

q59dilem3 Accept register all movements * CarBinary Car daily / less Crosstabulation[a]

			CarBinary Car daily / less		
			Less	Daily	Total
q59dilem3 Accept register all movements	no	Count	22	10	32
		% within CarBinary Car daily / less	95,7%	100,0%	97,0%
	yes	Count	1	0	1
		% within CarBinary Car daily / less	4,3%	,0%	3,0%
Total		Count	23	10	33
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = ES

q59dilem4 Accept only accidents * CarBinary Car daily / less Crosstabulation[a]

			CarBinary Car daily / less		
			Less	Daily	Total
q59dilem4 Accept only accidents	no	Count	16	7	23
		% within CarBinary Car daily / less	69,6%	70,0%	69,7%
	yes	Count	7	3	10
		% within CarBinary Car daily / less	30,4%	30,0%	30,3%
Total		Count	23	10	33
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = ES

q59dilem5 Accept only if voluntary * CarBinary Car daily / less Crosstabulation[a]

			CarBinary Car daily / less		
			Less	Daily	Total
q59dilem5 Accept only if voluntary	no	Count	11	7	18
		% within CarBinary Car daily / less	47,8%	70,0%	54,5%
	yes	Count	12	3	15
		% within CarBinary Car daily / less	52,2%	30,0%	45,5%
Total		Count	23	10	33
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = ES

q59dilem6 d.k. * CarBinary Car daily / less Crosstabulation[a]

		CarBinary Car daily / less		
		Less	Daily	Total
q59dilem6 d.k. no	Count	23	10	33
	% within CarBinary Car daily / less	100,0%	100,0%	100,0%
Total	Count	23	10	33
	% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = ES

10) Crosstabulations – Communications (phone and internet)

q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary * PhoneBinary Phone daily / less Crosstabulation[a]

			PhoneBinary Phone daily / less		
			Less	Daily	Total
q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary	completely agree	Count	1	8	9
		% within PhoneBinary Phone daily / less	33,3%	26,7%	27,3%
	partly agree	Count	1	8	9
		% within PhoneBinary Phone daily / less	33,3%	26,7%	27,3%
	neither agree nor disagree	Count	0	3	3
		% within PhoneBinary Phone daily / less	,0%	10,0%	9,1%
	partly disagree	Count	1	9	10
		% within PhoneBinary Phone daily / less	33,3%	30,0%	30,3%
	completely disagree	Count	0	2	2
		% within PhoneBinary Phone daily / less	,0%	6,7%	6,1%
Total		Count	3	30	33
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = ES

43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary * EmailBinary Email daily / less Crosstabulation[a]

			EmailBinary Email daily / less		
			Less	Daily	Total
q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary	completely agree	Count	9	0	9
		% within EmailBinary Email daily / less	39,1%	,0%	27,3%
	partly agree	Count	4	5	9
		% within EmailBinary Email daily / less	17,4%	50,0%	27,3%
	neither agree nor disagree	Count	3	0	3
		% within EmailBinary Email daily / less	13,0%	,0%	9,1%
	partly disagree	Count	5	5	10
		% within EmailBinary Email daily / less	21,7%	50,0%	30,3%
	completely disagree	Count	2	0	2
		% within EmailBinary Email daily / less	8,7%	,0%	6,1%
Total		Count	23	10	33
		% within EmailBinary Email daily / less	100,0%	100,0%	100,0%

a. country = ES

q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary * InternetBinary Internet daily / less Crosstabulation[a]

			InternetBinary Internet daily / less		
			Less	Daily	Total
q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary	completely agree	Count	8	1	9
		% within InternetBinary Internet daily / less	47,1%	6,3%	27,3%
	partly agree	Count	3	6	9
		% within InternetBinary Internet daily / less	17,6%	37,5%	27,3%
	neither agree nor disagree	Count	3	0	3
		% within InternetBinary Internet daily / less	17,6%	,0%	9,1%
	partly disagree	Count	2	8	10
		% within InternetBinary Internet daily / less	11,8%	50,0%	30,3%
	completely disagree	Count	1	1	2
		% within InternetBinary Internet daily / less	5,9%	6,3%	6,1%
Total		Count	17	16	33
		% within InternetBinary Internet daily / less	100,0%	100,0%	100,0%

a. country = ES

¡44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes * PhoneBinary Phone daily / less Crosstabulation[a]

			PhoneBinary Phone daily / less		
			Less	Daily	Total
q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes	completely agree	Count	1	14	15
		% within PhoneBinary Phone daily / less	33,3%	46,7%	45,5%
	partly agree	Count	1	8	9
		% within PhoneBinary Phone daily / less	33,3%	26,7%	27,3%
	neither agree nor disagree	Count	1	4	5
		% within PhoneBinary Phone daily / less	33,3%	13,3%	15,2%
	partly disagree	Count	0	3	3
		% within PhoneBinary Phone daily / less	,0%	10,0%	9,1%
	completely disagree	Count	0	1	1
		% within PhoneBinary Phone daily / less	,0%	3,3%	3,0%
Total		Count	3	30	33
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = ES

44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes * EmailBinary Email daily / less Crosstabulation[a]

			EmailBinary Email daily / less		
			Less	Daily	Total
q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes	completely agree	Count	10	5	15
		% within EmailBinary Email daily / less	43,5%	50,0%	45,5%
	partly agree	Count	6	3	9
		% within EmailBinary Email daily / less	26,1%	30,0%	27,3%
	neither agree nor disagree	Count	4	1	5
		% within EmailBinary Email daily / less	17,4%	10,0%	15,2%
	partly disagree	Count	2	1	3
		% within EmailBinary Email daily / less	8,7%	10,0%	9,1%
	completely disagree	Count	1	0	1
		% within EmailBinary Email daily / less	4,3%	,0%	3,0%
Total		Count	23	10	33
		% within EmailBinary Email daily / less	100,0%	100,0%	100,0%

a. country = ES

q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes * InternetBinary Internet daily / less Crosstabulation[a]

			InternetBinary Internet daily / less		
			Less	Daily	Total
q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes	completely agree	Count	7	8	15
		% within InternetBinary Internet daily / less	41,2%	50,0%	45,5%
	partly agree	Count	4	5	9
		% within InternetBinary Internet daily / less	23,5%	31,3%	27,3%
	neither agree nor disagree	Count	3	2	5
		% within InternetBinary Internet daily / less	17,6%	12,5%	15,2%
	partly disagree	Count	2	1	3
		% within InternetBinary Internet daily / less	11,8%	6,3%	9,1%
	completely disagree	Count	1	0	1
		% within InternetBinary Internet daily / less	5,9%	,0%	3,0%
Total		Count	17	16	33
		% within InternetBinary Internet daily / less	100,0%	100,0%	100,0%

a. country = ES

q45data Scanning of and combining data from different databases containing personal information is privacy infringing * PhoneBinary Phone daily / less Crosstabulation[a]

			PhoneBinary Phone daily / less		
			Less	Daily	Total
q45data Scanning of and combining data from different databases containing personal information is privacy infringing	completely agree	Count	2	15	17
		% within PhoneBinary Phone daily / less	66,7%	50,0%	51,5%
	partly agree	Count	1	7	8
		% within PhoneBinary Phone daily / less	33,3%	23,3%	24,2%
	neither agree nor disagree	Count	0	4	4
		% within PhoneBinary Phone daily / less	,0%	13,3%	12,1%
	partly disagree	Count	0	3	3
		% within PhoneBinary Phone daily / less	,0%	10,0%	9,1%
	completely disagree	Count	0	1	1
		% within PhoneBinary Phone daily / less	,0%	3,3%	3,0%
Total		Count	3	30	33
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = ES

45data Scanning of and combining data from different databases containing personal information is privac infringing * EmailBinary Email daily / less Crosstabulation[a]

			EmailBinary Email daily / less		
			Less	Daily	Total
q45data Scanning of and combining data from different databases containing personal information is privacy infringing	completely agree	Count	10	7	17
		% within EmailBinary Email daily / less	43,5%	70,0%	51,5%
	partly agree	Count	6	2	8
		% within EmailBinary Email daily / less	26,1%	20,0%	24,2%
	neither agree nor disagree	Count	4	0	4
		% within EmailBinary Email daily / less	17,4%	,0%	12,1%
	partly disagree	Count	2	1	3
		% within EmailBinary Email daily / less	8,7%	10,0%	9,1%
	completely disagree	Count	1	0	1
		% within EmailBinary Email daily / less	4,3%	,0%	3,0%
Total		Count	23	10	33
		% within EmailBinary Email daily / less	100,0%	100,0%	100,0%

a. country = ES

q45data Scanning of and combining data from different databases containing personal information is privacy infringing * InternetBinary Internet daily / less Crosstabulation[a]

			InternetBinary Internet daily / less		
			Less	Daily	Total
q45data Scanning of and combining data from different databases containing personal information is privacy infringing	completely agree	Count	7	10	17
		% within InternetBinary Internet daily / less	41,2%	62,5%	51,5%
	partly agree	Count	4	4	8
		% within InternetBinary Internet daily / less	23,5%	25,0%	24,2%
	neither agree nor disagree	Count	3	1	4
		% within InternetBinary Internet daily / less	17,6%	6,3%	12,1%
	partly disagree	Count	2	1	3
		% within InternetBinary Internet daily / less	11,8%	6,3%	9,1%
	completely disagree	Count	1	0	1
		% within InternetBinary Internet daily / less	5,9%	,0%	3,0%
Total		Count	17	16	33
		% within InternetBinary Internet daily / less	100,0%	100,0%	100,0%

a. country = ES

q47data Databases being used for something else than the original purpose is a serious privacy problem * PhoneBinary Phone daily / less Crosstabulation[a]

			PhoneBinary Phone daily / less		
			Less	Daily	Total
q47data Databases being used for something else than the original purpose is a serious privacy problem	0	Count	0	1	1
		% within PhoneBinary Phone daily / less	,0%	3,3%	3,0%
	completely agree	Count	3	23	26
		% within PhoneBinary Phone daily / less	100,0%	76,7%	78,8%
	partly agree	Count	0	1	1
		% within PhoneBinary Phone daily / less	,0%	3,3%	3,0%
	neither agree nor disagree	Count	0	1	1
		% within PhoneBinary Phone daily / less	,0%	3,3%	3,0%
	partly disagree	Count	0	1	1
		% within PhoneBinary Phone daily / less	,0%	3,3%	3,0%
	completely disagree	Count	0	3	3
		% within PhoneBinary Phone daily / less	,0%	10,0%	9,1%
Total		Count	3	30	33
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = ES

q47data Databases being used for something else than the original purpose is a serious privacy problem * EmailBinary Email daily / less Crosstabulation[a]

			EmailBinary Email daily / less		
			Less	Daily	Total
q47data Databases being used for something else than the original purpose is a serious privacy problem	0	Count	1	0	1
		% within EmailBinary Email daily / less	4,3%	,0%	3,0%
	completely agree	Count	18	8	26
		% within EmailBinary Email daily / less	78,3%	80,0%	78,8%
	partly agree	Count	0	1	1
		% within EmailBinary Email daily / less	,0%	10,0%	3,0%
	neither agree nor disagree	Count	1	0	1
		% within EmailBinary Email daily / less	4,3%	,0%	3,0%
	partly disagree	Count	1	0	1
		% within EmailBinary Email daily / less	4,3%	,0%	3,0%
	completely disagree	Count	2	1	3
		% within EmailBinary Email daily / less	8,7%	10,0%	9,1%
Total		Count	23	10	33
		% within EmailBinary Email daily / less	100,0%	100,0%	100,0%

a. country = ES

q47data Databases being used for something else than the original purpose is a serious privacy problem * InternetBinary Internet daily / less Crosstabulation[a]

			InternetBinary Internet daily / less		
			Less	Daily	Total
q47data Databases being used for something else than the original purpose is a serious privacy problem	0	Count	0	1	1
		% within InternetBinary Internet daily / less	,0%	6,3%	3,0%
	completely agree	Count	13	13	26
		% within InternetBinary Internet daily / less	76,5%	81,3%	78,8%
	partly agree	Count	0	1	1
		% within InternetBinary Internet daily / less	,0%	6,3%	3,0%
	neither agree nor disagree	Count	1	0	1
		% within InternetBinary Internet daily / less	5,9%	,0%	3,0%
	partly disagree	Count	1	0	1
		% within InternetBinary Internet daily / less	5,9%	,0%	3,0%
	completely disagree	Count	2	1	3
		% within InternetBinary Internet daily / less	11,8%	6,3%	9,1%
Total		Count	17	16	33
		% within InternetBinary Internet daily / less	100,0%	100,0%	100,0%

a. country = ES

q51wire Eavesdropping is a serious violation of privacy * PhoneBinary Phone daily / less Crosstabulation[a]

			PhoneBinary Phone daily / less		
			Less	Daily	Total
q51wire Eavesdropping is a serious violation of privacy	completely agree	Count	2	13	15
		% within PhoneBinary Phone daily / less	66,7%	43,3%	45,5%
	partly agree	Count	1	14	15
		% within PhoneBinary Phone daily / less	33,3%	46,7%	45,5%
	neither agree nor disagree	Count	0	1	1
		% within PhoneBinary Phone daily / less	,0%	3,3%	3,0%
	partly disagree	Count	0	1	1
		% within PhoneBinary Phone daily / less	,0%	3,3%	3,0%
	completely disagree	Count	0	1	1
		% within PhoneBinary Phone daily / less	,0%	3,3%	3,0%
Total		Count	3	30	33
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = ES

q51wire Eavesdropping is a serious violation of privacy * EmailBinary Email daily / less Crosstabulation[a]

			EmailBinary Email daily / less		
			Less	Daily	Total
q51wire Eavesdropping is a serious violation of privacy	completely agree	Count	8	7	15
		% within EmailBinary Email daily / less	34,8%	70,0%	45,5%
	partly agree	Count	13	2	15
		% within EmailBinary Email daily / less	56,5%	20,0%	45,5%
	neither agree nor disagree	Count	0	1	1
		% within EmailBinary Email daily / less	,0%	10,0%	3,0%
	partly disagree	Count	1	0	1
		% within EmailBinary Email daily / less	4,3%	,0%	3,0%
	completely disagree	Count	1	0	1
		% within EmailBinary Email daily / less	4,3%	,0%	3,0%
Total		Count	23	10	33
		% within EmailBinary Email daily / less	100,0%	100,0%	100,0%

a. country = ES

q51wire Eavesdropping is a serious violation of privacy * InternetBinary Internet daily / less Crosstabulation[a]

			InternetBinary Internet daily / less		
			Less	Daily	Total
q51wire Eavesdropping is a serious violation of privacy	completely agree	Count	6	9	15
		% within InternetBinary Internet daily / less	35,3%	56,3%	45,5%
	partly agree	Count	9	6	15
		% within InternetBinary Internet daily / less	52,9%	37,5%	45,5%
	neither agree nor disagree	Count	0	1	1
		% within InternetBinary Internet daily / less	,0%	6,3%	3,0%
	partly disagree	Count	1	0	1
		% within InternetBinary Internet daily / less	5,9%	,0%	3,0%
	completely disagree	Count	1	0	1
		% within InternetBinary Internet daily / less	5,9%	,0%	3,0%
Total		Count	17	16	33
		% within InternetBinary Internet daily / less	100,0%	100,0%	100,0%

a. country = ES

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy * PhoneBinary Phone daily / less Crosstabulation[a]

			PhoneBinary Phone daily / less		
			Less	Daily	Total
q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy	completely agree	Count	2	15	17
		% within PhoneBinary Phone daily / less	66,7%	50,0%	51,5%
	partly agree	Count	0	6	6
		% within PhoneBinary Phone daily / less	,0%	20,0%	18,2%
	neither agree nor disagree	Count	1	7	8
		% within PhoneBinary Phone daily / less	33,3%	23,3%	24,2%
	partly disagree	Count	0	2	2
		% within PhoneBinary Phone daily / less	,0%	6,7%	6,1%
Total		Count	3	30	33
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = ES

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy * EmailBinary Email daily / less Crosstabulation[a]

			EmailBinary Email daily / less		
			Less	Daily	Total
q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy	completely agree	Count	12	5	17
		% within EmailBinary Email daily / less	52,2%	50,0%	51,5%
	partly agree	Count	3	3	6
		% within EmailBinary Email daily / less	13,0%	30,0%	18,2%
	neither agree nor disagree	Count	6	2	8
		% within EmailBinary Email daily / less	26,1%	20,0%	24,2%
	partly disagree	Count	2	0	2
		% within EmailBinary Email daily / less	8,7%	,0%	6,1%
Total		Count	23	10	33
		% within EmailBinary Email daily / less	100,0%	100,0%	100,0%

a. country = ES

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy * InternetBinary Internet daily / less Crosstabulation[a]

			InternetBinary Internet daily / less		
			Less	Daily	Total
q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy	completely agree	Count	10	7	17
		% within InternetBinary Internet daily / less	58,8%	43,8%	51,5%
	partly agree	Count	1	5	6
		% within InternetBinary Internet daily / less	5,9%	31,3%	18,2%
	neither agree nor disagree	Count	4	4	8
		% within InternetBinary Internet daily / less	23,5%	25,0%	24,2%
	partly disagree	Count	2	0	2
		% within InternetBinary Internet daily / less	11,8%	,0%	6,1%
Total		Count	17	16	33
		% within InternetBinary Internet daily / less	100,0%	100,0%	100,0%

a. country = ES

q58dilem1 Accept all access for counter terrorism * PhoneBinary Phone daily / less Crosstabulation[a]

			PhoneBinary Phone daily / less		
			Less	Daily	Total
q58dilem1 Accept all access for counter terrorism	no	Count	2	20	22
		% within PhoneBinary Phone daily / less	66,7%	66,7%	66,7%
	yes	Count	1	10	11
		% within PhoneBinary Phone daily / less	33,3%	33,3%	33,3%
Total		Count	3	30	33
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = ES

q58dilem1 Accept all access for counter terrorism * EmailBinary Email daily / less Crosstabulation[a]

			EmailBinary Email daily / less		
			Less	Daily	Total
q58dilem1 Accept all access for counter terrorism	no	Count	14	8	22
		% within EmailBinary Email daily / less	60,9%	80,0%	66,7%
	yes	Count	9	2	11
		% within EmailBinary Email daily / less	39,1%	20,0%	33,3%
Total		Count	23	10	33
		% within EmailBinary Email daily / less	100,0%	100,0%	100,0%

a. country = ES

q58dilem1 Accept all access for counter terrorism * InternetBinary Internet daily / less Crosstabulation[a]

			InternetBinary Internet daily / less		
			Less	Daily	Total
q58dilem1 Accept all access for counter terrorism	no	Count	9	13	22
		% within InternetBinary Internet daily / less	52,9%	81,3%	66,7%
	yes	Count	8	3	11
		% within InternetBinary Internet daily / less	47,1%	18,8%	33,3%
Total		Count	17	16	33
		% within InternetBinary Internet daily / less	100,0%	100,0%	100,0%

a. country = ES

q34local1 Terrorists and criminals w court order * PhoneBinary Phone daily / less Crosstabulation[a]

			PhoneBinary Phone daily / less		
			Less	Daily	Total
q34local1 Terrorists and criminals w court order	no	Count	0	9	9
		% within PhoneBinary Phone daily / less	,0%	30,0%	27,3%
	yes	Count	3	21	24
		% within PhoneBinary Phone daily / less	100,0%	70,0%	72,7%
Total		Count	3	30	33
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = ES

q34local2 Any w/o court order * PhoneBinary Phone daily / less Crosstabulation[a]

			PhoneBinary Phone daily / less		
			Less	Daily	Total
q34local2 Any w/o court order	no	Count	3	27	30
		% within PhoneBinary Phone daily / less	100,0%	90,0%	90,9%
	yes	Count	0	3	3
		% within PhoneBinary Phone daily / less	,0%	10,0%	9,1%
Total		Count	3	30	33
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = ES

q34local3 Emergency * PhoneBinary Phone daily / less Crosstabulation[a]

			PhoneBinary Phone daily / less		
			Less	Daily	Total
q34local3 Emergency	no	Count	0	3	3
		% within PhoneBinary Phone daily / less	,0%	10,0%	9,1%
	yes	Count	3	27	30
		% within PhoneBinary Phone daily / less	100,0%	90,0%	90,9%
Total		Count	3	30	33
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = ES

q34local4 Never * PhoneBinary Phone daily / less Crosstabulation[a]

			PhoneBinary Phone daily / less		
			Less	Daily	Total
q34local4 Never	no	Count	3	29	32
		% within PhoneBinary Phone daily / less	100,0%	96,7%	97,0%
	yes	Count	0	1	1
		% within PhoneBinary Phone daily / less	,0%	3,3%	3,0%
Total		Count	3	30	33
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = ES

q34local5 d.k. * PhoneBinary Phone daily / less Crosstabulation[a]

		PhoneBinary Phone daily / less		
		Less	Daily	Total
q34local5 d.k. no	Count	3	30	33
	% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%
Total	Count	3	30	33
	% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = ES

q52protect1 Anonymous calling cards * PhoneBinary Phone daily / less Crosstabulation[a]

			PhoneBinary Phone daily / less		
			Less	Daily	Total
q52protect1 Anonymous calling cards	no	Count	2	21	23
		% within PhoneBinary Phone daily / less	66,7%	70,0%	69,7%
	yes	Count	1	9	10
		% within PhoneBinary Phone daily / less	33,3%	30,0%	30,3%
Total		Count	3	30	33
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = ES

q37local The possibility of locating all mobile phones is privacy infringing * PhoneBinary Phone daily / less Crosstabulation[a]

			PhoneBinary Phone daily / less		
			Less	Daily	Total
q37local The possibility of locating all mobile phones is privacy infringing	completely agree	Count	2	14	16
		% within PhoneBinary Phone daily / less	66,7%	46,7%	48,5%
	partly agree	Count	1	9	10
		% within PhoneBinary Phone daily / less	33,3%	30,0%	30,3%
	neither agree nor disagree	Count	0	2	2
		% within PhoneBinary Phone daily / less	,0%	6,7%	6,1%
	partly disagree	Count	0	2	2
		% within PhoneBinary Phone daily / less	,0%	6,7%	6,1%
	completely disagree	Count	0	3	3
		% within PhoneBinary Phone daily / less	,0%	10,0%	9,1%
Total		Count	3	30	33
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = ES

q52protect2 Encryption programmes * EmailBinary Email daily / less Crosstabulation[a]

			EmailBinary Email daily / less		
			Less	Daily	Total
q52protect2 Encryption programmes	no	Count	13	5	18
		% within EmailBinary Email daily / less	56,5%	50,0%	54,5%
	yes	Count	10	5	15
		% within EmailBinary Email daily / less	43,5%	50,0%	45,5%
Total		Count	23	10	33
		% within EmailBinary Email daily / less	100,0%	100,0%	100,0%

a. country = ES

q52protect3 Identity management * InternetBinary Internet daily / less Crosstabulation[a]

			InternetBinary Internet daily / less		
			Less	Daily	Total
q52protect3 Identity management	no	Count	11	9	20
		% within InternetBinary Internet daily / less	64,7%	56,3%	60,6%
	yes	Count	6	7	13
		% within InternetBinary Internet daily / less	35,3%	43,8%	39,4%
Total		Count	17	16	33
		% within InternetBinary Internet daily / less	100,0%	100,0%	100,0%

a. country = ES

ANNEX V

Comments from the questionnaire

1) I believe that we should also think about other types of security such as the one relatef to violence against women.
2) As long as these measures are reliable and do not create too many problems for daily life, it is acceptable to violate privacy in this way some criminal act maybe prevented.
3) I think it is right to make research on new security technologies but I think these should not focus merely on fighting terrorism because there are many others things that threaten public security. In addition, we should begin to use correctly the tecnologies that are already available.
4) The debate suggested is of difficul solution, because (the tecnologies) may invade a right that is intrisic to the person, such as the right to privacy that is an individual right.
5) the issues are too complicated to express an opinion in such a short time, it is necessary to think more and to have more social awareness, there is debate about this. There are some questions that I did not understand whilst some other were actually pointing at a specific answer, or maybe the answers were not consistent with my opinion, therefore my answers in some occasions have been approximated.
6) The knowledge of security technology is crucial, because its implementation in various aspects will produce a a feeling of security and prevention of phenomena like terrorism and criminality.
7) In general terms, I disagree with the use of these technologies, because I don´t belive that these technolgies work (It is not possible the control of every criminal act).
8) Analyze risks of all types, especially for the health (x-rays), for commercial purposes and in relation to the violation of private life
9) I would like to add that it is very difficult that everybody agrees; because something is good for one and bad for other.
10) I think that all security technology that violate privacy should be optional, that is to say the individual should be free to use . Security should always implemented in order to offer the advantage or the reward to those who use it and disadvantages to those who do no t make use of it. When there is a risk of privact violation, a judge should always have the responsibility to decide.
11) I think that as long as people that have nothing to hide security technologies are very important in our daily life. They bring a lot of more peace. I am in favour of security technologies