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

Illustrated Scenarios – Spanish Version

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

Author(s): Christine Hafskjold, The Norwegian Board of Technology
Translation: Vincenzo Pavone, CSIC Unit of Comparative Policy and Politics
Illustrations: Åsne Flyen

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

Table of Contents **page**

Preface

The **PRISE**-project aims at contributing to a secure future for the European Union consistent with European citizens' civil rights - in particular privacy – and their preferences.
The project will:

- Develop criteria and guidelines for privacy compliant security research and technology development.
- Transform the results into scenarios that present applications of security technologies and measures that comply with civil rights and privacy to a varying degree.
- Test these scenarios in a set of participatory technology assessment procedures in different European states, allowing for a substantiated indication of public perception and citizens' preferences.
- Elaborate the sets of criteria and guidelines with direct involvement of providers of security technologies, private and public users and implementers, institutions and bodies shaping policies and regulation as well as organisations representing potentially and actually conflicting interests.
- Disseminate the results to actors relevant for the shaping of technologies and policies.

This document is a presentation of the scenarios developed in Work Package 4. Before being presented to the groups of lay people in different European states, the scenarios will be translated into their native language. The scenarios aim at giving the lay people insight into different security technologies and how they can be applied in everyday life in a near future. We try to address different approaches to the technologies, both from a user point of view, and in the society.
The technical descriptions in this document are adapted from *D 2.2 Overview of Security Technologies*.
The PRISE project would like to thank the group of experts that have helped us in developing the scenarios:

Asle Fossberg, The National Police Computing and Material Service

Marit Gjerde, The Norwegian Police University College

Nina Græger, Norwegian Institute of International Affairs

Ove Skåra, The Norwegian Data Inspectorate

Thomas Olsen, Norwegian Research Center for Computers and Law

We would also like to thank Jordi Mas, Deputy Director of the Catalan Foundation for Research and Innovation, who has been kind enough to provide feedback on the scenarios during the process.

Introduction

This document will present you with some scenarios showing how security technologies and surveillance may be used in everyday situations – in the near future.

What is security technology?

Security can be defined as the absence of danger – that is a state where the desired status quo is not threatened or disrupted in any way. In the context of the **PRISE** project, security is understood as the security of the society – or more precisely – of the citizens that constitute the society.
The term *security technology* can cover everything from private alarm systems and virus protection systems for PCs to border control systems and international police co-operation. In our scenarios we mainly focus on technologies or means (systems, legislation etc.) that are meant to enhance the security of the society against threats from individuals, or groups of individuals (not from states). This covers crime-fighting, anti-terror activities, border control activities etc.
In the scenario text we introduce some facts about the different technologies, to help you understand how they work today and their potential for the future.

What is privacy?

Privacy is generally associated with the protection of the integrity, autonomy and private life of the individual. Basically, it's about people's right to choose how they want to live their life, and what things they want to keep private. Privacy is considered a basic human right, and the first regulation of privacy is article 12 in the Universal Declaration of Human Rights.
What makes the protection of privacy difficult is the fact that privacy is almost always competing against other goods in society, such as mobility, efficiency, security or convenience. For example; even if we know that carrying a mobile phone that is turned on makes it possible to trace where we are, most of us would not dream of leaving the phone at home! And most people prefer having an RFID token in their car, rather than waiting in line to pay with (anonymous) cash when driving onto a toll-road.
Research suggests that many people are not concerned about technologies that infringe their privacy because they feel they have nothing to hide. Experts fear that this will result in a loss in privacy for the society that can be difficult to regain once it is gone. And even the most law-abiding citizen may find himself in a situation where he wouldn't want to be watched or traced.
When it comes to security technologies and surveillance, critics claim that a lot of the measures that are implemented are not suited to combat terror, but only to reassure the public that "something is being done". This is because the measures can be circumvented or because the threat they address is too unlikely to justify the action taken against it. A much used example of this is the banning of anonymous calling cards in many countries. Critics of this ban claim that it only stops ordinary people who would like to be anonymous; the criminals have ways of circumventing it by registering with a fake identity or using stolen mobile phones.
Some of the anti-terror initiatives, in particular in the United States, are very privacy infringing, such as eavesdropping telephone calls, screening electronic communication without a warrant or analysing someone based on data collected from different sources without informing the person in question.
An important privacy principle is that a person should be informed when his or her personal data is stored and processed, and that it is possible to get access to the data and

check that it is correct. Personal data should only be collected and stored if it is really necessary and it should be deleted when it is no longer needed for the original purpose.

¿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.

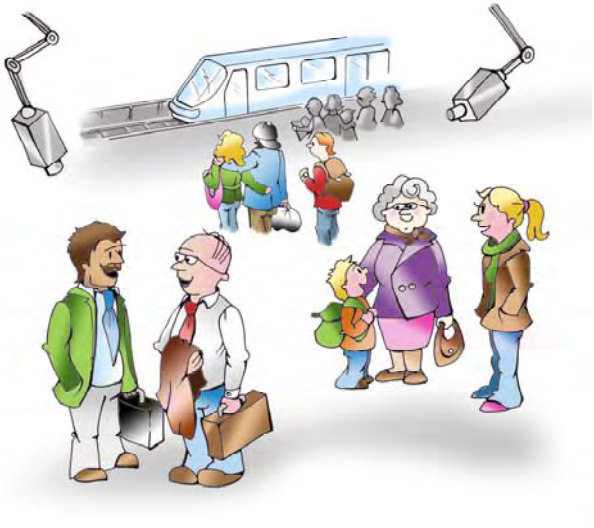
Últimamente, cada vez más gente cuestiona la legitimidad y la eficiencia de las cámaras. En algunas zonas de la ciudad están realizando pruebas en las que, en lugar de cámaras de vigilancia, instalan una iluminación mejor y más intensa, ¡al parecer con buenos resultados!

- 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.

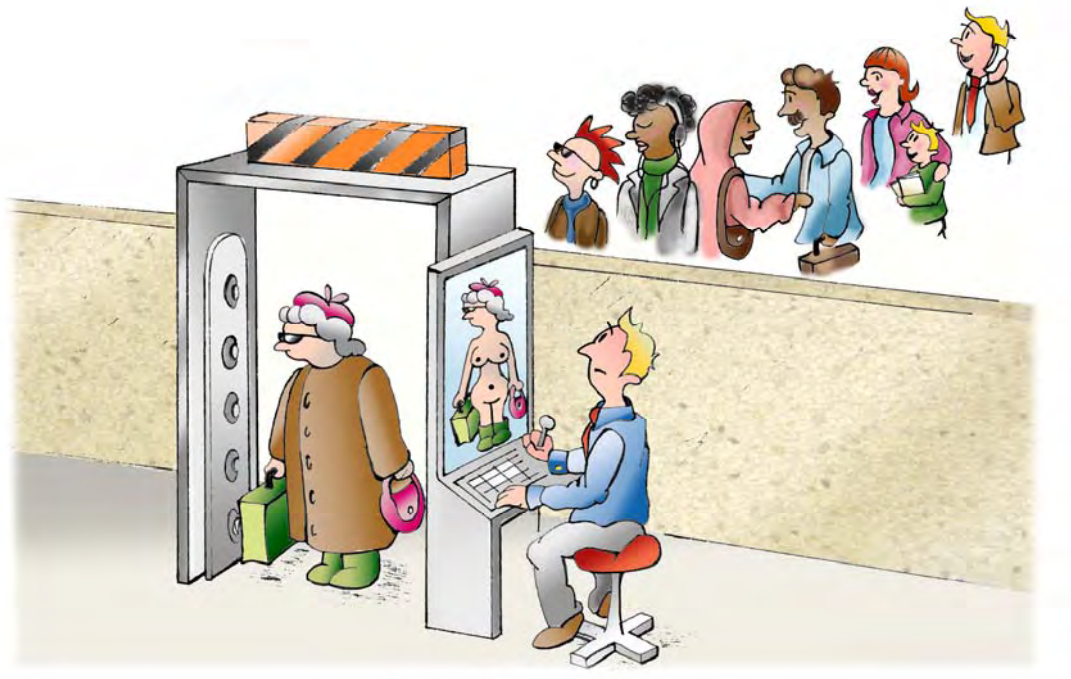
Últimamente hemos observado una tendencia en la que los gobiernos han pretendido almacenar más información y conectar los sistemas de bases de datos con fines distintos del original, como la seguridad. El tipo de datos a los que más se alude cuando se debate la retención de datos son los relacionados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

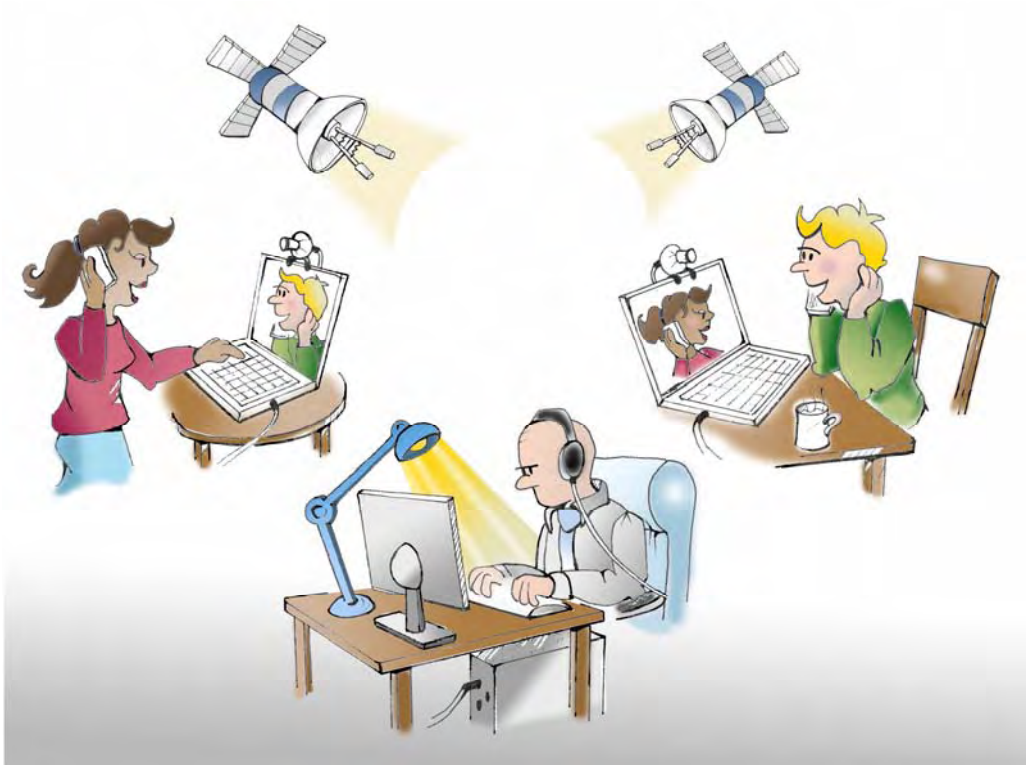
Una versión ampliada de las escuchas es pinchar de forma más indiscriminada todas las líneas de comunicación (teléfono, móvil e Internet) en busca de conversaciones que puedan resultar de interés. Un ejemplo de esto es la red Echelon, dirigida por una alianza entre EE UU, Reino Unido, Canadá, Australia 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"…