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 – Hungarian Version

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

Author(s): Christine Hafskjold, The Norwegian Board of Technology
Translation: Eszter Bakonyi, Median
Illustrations: Åsne Flyen

Classification: Public

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.

1.1 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.

1.2 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.

Mi a véleménye a különböző biztonságtechnikákról? Vitaindító forgatókönyvek

A következő részben két emberről, Kláráról és Péterről mutatunk be Önnek néhány történetet. Nyomon követjük találkozásaikat a különféle biztonságtechnikákkal és eszközökkel, majd megismerjük gondolataikat és véleményüket ezekkel kapcsolatban. A példák általánossága kedvéért a történetekben nem használtunk konkrét ország-, város- vagy repülőtérneveket, inkább azt igyekszünk bemutatni, hogyan alkalmaztak a különböző országok – biztonsági hatóságok – más-más megközelítést a biztonságtechnikák alkalmazása során. A forgatókönyvek a jövőben játszódnak annak érdekében, hogy olyan biztonságtechnikákat és törvényi szabályozásokat is be tudjunk mutatni a segítségükkel, amelyek ma még nincsenek érvényben.

Reméljük, a történetek segítenek Önnek eligazodni a biztonsággal és a magánélet védelmével kapcsolatban, és hogy megfogalmazza saját véleményét erről a két értékről.

Klára hatvankét éves. Egész életében tanárként dolgozott, de most azt fontolgatja, hogy hamar nyugdíjba vonul. Manapság már mindent elural a technika! Ráadásul mintha a gyerekek is zajosabbak lennének, mint régen. Biztosan öregszik. Ezen a héten azonban más foglalkoztatja. Éppen kezdődik a nyári szünet, és látogatóba megy a fiához az egyik szomszédos országba.

Klára metróval megy a központi vonatpályaudvarra. Előzőleg „feltöltötte” *Általános jegy* nevet viselő kártyáját, s azzal fizeti majd ki az utazását. Nem kell mást tennie, mint a jegyet a beolvasó eszköz elé tartania a pályaudvar beengedő kapujánál. A jegy tulajdonképpen egy mikrocsippel ellátott műanyag kártya. A csip nyilvántartja, hogy a kártya tulajdonosa mennyit utazhat még a kártyájával. Klára ún. anonim (névtelen) jegyet vásárolt. Tisztában van vele, ha elveszti a jegyet, a pénze is elvész, és a dolog még egy kis külön odafigyeléssel is jár a kártya használata miatt. A szokásos *általános jegy* természetesen bele van

építve a tulajdonos *hordozható egységébe.* Gazdájának nem kell mást tennie, mint magán viselni, vagy a pénztárcájában hordani a mobil egységet, és ujjlenyomatával igazolnia magát, amikor belép a kapun.

Klára nem tehet róla, de kellemetlennek találja a gondolatot, hogy az

ujjlenyomatával kelljen azonosítania magát. Természetesen látja, hogy a mai fiatalokat ez egyáltalán nem zavarja, neki azonban mindig a bűnözők és a letartóztatások jutnak az eszébe róla. „Már az is elég baj, hogy külföldi utazásnál kötelező ujjlenyomatot adni és felmutatni a személyi igazolványt” – gondolja. Határozottan úgy érzi, nem szeretné ezt többször megtenni, mint ahányszor most kénytelen.

Biometria

A biometrikus technika személyek automatikus azonosítására szolgál biológiai vagy viselkedésbeli jellemzők alapján. A biometrikus azonosítás segítségével korlátozható az adott személy valamilyen fizikai helyhez, illetve információhoz (számítógéphez, dokumentumhoz) való hozzáférési jogosultsága. A leggyakrabban alkalmazott biometrikus azonosítók közé tartoznak az ujjlenyomatok és az arc különböző jellemzői.

Azt a folyamatot, amelynek során egy személy biometrikus jellemzőit összehasonlítják az előzetesen tárolt sablonnal, illesztésnek nevezzük. Az illesztés eredménye egy ún. azonosságmérték. A személy elfogadása vagy elutasítása azon múlik, hogy ez a mérték meghaladja-e az adott határértéket.

A legtöbb esetben a biometrikus képet sablon formájában tárolják, ami a biometrikus jellemző digitális megfelelője. A sablon valamilyen algoritmus segítségével jön létre. A személyes adatok védelme szempontjából ajánlatos csupán a sablon tárolása, s az eredeti kép megsemmisítése. Ezzel szemben a végrehajtó hatóságok rendszereikben, például a biometrikus útlevélnél és az arcfelismerő rendszerekben gyakran az eredeti képet is megtartják.

Különbséget tehetünk biometrikus *azonosítás* és *hitelesítés* között. Az előbbi arra szolgál, hogy megállapítsuk az ellenőrzött személy személyazonosságát a tőle nyert sablon és a rendszerben tárolt összes sablon összehasonlításával. Az utóbbi során pedig a személyt a rendszerben tárolt saját sablonjával vetjük össze, hogy megállapíthassuk, az-e, akinek mondja magát.

A biometrikus azonosítás nehézsége a megfelelő arány megtalálása a „hamis elfogadási arány” (False Acceptance Rate: FAR) és a „hamis elutasítási arány” (False Rejection Rate: FRR) között. Az eredmény akkor számít hamis elfogadásnak (vagy hamis pozitívnak), amikor a rendszer helytelenül azonosítja az egyént. Vagyis annak ellenére, hogy az ő sablonja nincs az adatbázisban, mégis talál benne olyat, ami *jelentős mértékben* megegyezik (de mégsem azonos) az övével, így azt jelzi, hogy ő az adatbázisban van. Arra az esetre, amikor a rendszer nem tud azonosítani egy már regisztrált személyt, a hamis elutasítás (hamis negatív) megjelölést használjuk.

A biometrikus azonosítás egyik fő előnye, hogy nagyon szorosan kapcsolódik az azonosítandó személyhez. A biometrikus hitelesítés hatékonyabbá teszi a hozzáférés-ellenőrzést, megnehezíti a más adataival való visszaéléseket (identitáslopás), mivel a személyes adatok kizárólagosan a megfelelő személyhez kacsolódnak (személyes azonosítókkal védett). Ugyanakkor a biometrikus rendszerek legnagyobb veszélye is ebben áll. Ha egy biometrikus adatsor egyszer rossz hírbe keveredik, az örökre szól.

Péter harminckét éves. Üzletkötő egy autókereskedésben. Ma reggel korán kel, mert egy autókiállításra utazik Közép-Európába. Felkel, gyorsan lezuhanyzik, fogja az utazótáskáját, beül az autójába, és elindul a reptér felé. Szokás szerint késésben van, de mivel bejelentkezett a

gyors sávra, még eléri a gépet. Az ún. gyors sáv lehetővé teszi, hogy elkerülje a reptéri bejelentkezéssel járó bonyodalmakat, amelynek során ellenőrzik, hogy az utas nem szerepel-e a nyilvántartott bűnözők adattárában, megnézik az útlevelet, majd természetesen átesik a szigorú biztonsági ellenőrzésen. A gyors sávra bejelentkezőnek mindössze egyszer kell átesnie egy különösen szigorú regisztrációs folyamaton, s engedélyeznie kell, hogy a reptér az összes adatát tárolja. Cserébe elkerülheti a felszállás előtti szokásos bejelentkezési eljárást, csupán a beengedő kapunál a biometrikus technika eszközeivel kell igazolnia magát.

Eszébe jut munkatársa, aki Péter véleménye szerint megszállottan ragaszkodik személyes adatai védelméhez. Szerinte már így is túl sok a felügyelet a társadalomban, s ma már a „sütiket” (vagy „jelszó és naplózó fájlokat”) sem engedi be a számítógépébe, azaz nem engedi, hogy az adatait tárolják! Még a Google eszközsávot is kitörölte a gépéből! Ki hallott már ilyet! Ha igaz lenne a híresztelés, mely szerint az amerikai ügynökségek ezek segítségével próbálják feltérképezni a hálózatokat és kiszűrni a gyanús alakokat, akkor ezt egészen biztosan mindenki tudná. Ebben a pillanatban azonban a munkatársa már néhány órája talpon van, és ott várakozik a reptéri sorban a bejelentkezéshez és a biztonsági ellenőrzéshez. Magának köszönheti! Péter csak remélni tudja, hogy a munkatársa időben átjut az ellenőrzésen ahhoz, hogy még egyszer utoljára átfussák az előadásukat beszállás előtt.

- o -

Klára megérkezik a központi vonatpályaudvarra. Itt is mindenütt kamerák vannak ugyanúgy, mint a metróban. A falakon kivetítők és hangosbemondók ismételgetik a biztonsági figyelmeztetéseket, már nem is figyel rájuk senki. „Ne hagyja őrizetlenül a csomagjait!” „Az Önről készült képet összevetjük az ismert terroristák adatbázisával.” Ez utóbbiról vita robbant ki néhány évvel ezelőtt. Sok országban nem tudatják az emberekkel nyilvánosan, hogy felvételek készülnek róluk, amiket aztán különböző adatbázisokkal hasonlítanak össze. Voltak, akik szerint ezt itt sem kellene nyilvánosan bejelenteni. A kormány azonban egyértelműen amellett foglalt állást, hogy az embereknek jogukban áll tudni, hogy mikor és hol ellenőrzik őket. „Ez különösen akkor fontos, ha nincs más mód arra, hogy észrevegyük. Igazából már nem is tudhatjuk, mikor készítenek rólunk felvételeket” – gondolja Klára. Hallotta, hogy vannak országok, ahol még az emberek elektronikus levelezését és telefonbeszélgetésit is szűrik gyanús szavak és kifejezések után. De ez már biztos csak szóbeszéd!

Klárának zúg a feje a sok zajtól, ezért elindul a *csendes zóna* felé. A belépéshez fel kell mutatnia a személyi igazolványát, de amint belép, megnyugszik. „Nincsenek kamerák, mobiltelefonok, vezeték nélküli eszközök, sőt hangos figyelmeztetések sem. Igazán több ilyen technikamentes zóna lehetne” – gondolja.

Nem mintha nem lenne hozzászokva a kamerákhoz. Csaknem egész felnőtt korában körülvették, mégis az utóbbi időben mintha tolakodóbbnak érezné őket. Mióta elkezdtek arc- és sablonfelismerő szoftvereket használni, sokkal inkább érzi, hogy megfigyelés alatt áll, mint korábban. „Nem úgy viselkedem éppen, mint egy terrorista?” Milyen kínos lenne, ha valami olyat tenne, ami miatt megállítaná és ellenőrizné őt a terrorelhárító rendőrség! Valójában még soha nem állították meg, de nem tud nem gondolni erre, amikor kamerák veszik körül.

Ráadásul a legtöbb emberhez hasonlóan ő is ismer valakit, akit ártatlanul terroristának néztek. A technika alkalmazásának korai időszakában sok gond volt az arcfelismerő

szoftverrel. S mivel a politikusok nem szerettek volna olyan botrányt, hogy a megfigyelési listán szereplők bármelyike kijátssza a rendszert, sok ún. „hamis pozitív” eredményű azonosítás történt.

Egyik munkatársát, akinek a szülei Iránból származnak, terroristának nézték. A férfi nagyon megszégyenítőnek érezte a helyzetet, és Klára ezt meg is érti. Ahogy a munkatársa mondta: „Ha úgy nézel ki, mint én és golyóálló mellénybe öltözött terrorelhárító rendőrök letartóztatnak, az emberek másként néznek rád utána, nem számít, hogy a rendőrök a végén elnézést kérnek tőled a tévedés miatt”. Klára tudta, hogy a munkatársa az eset után egy ideig kerülte az erősen bekamerázott környékeket, különösen akkor, amikor a gyerekei is vele voltak.

Az utóbbi időben egyre több ember kérdőjelezi meg mind a kamerák jogosságát, mind a hatékonyságát. A város egyes részein az utcákat megfigyelő kamerák helyett jobb megvilágítással látták el. Szemmel láthatóan kedvezőek a tapasztalatok.

- o -

Péter autója, mivel autókereskedésben dolgozik, mindig a legújabb modellek közül való. Az autó, amit ebben a pillanatban vezet, a legújabb technikával van felszerelve: van benne Galileo műholdas helymeghatározó rendszer, automatikus segélyhívó az eCall rendszeren keresztül, és egy csokor egyéb járműbiztonsági rendszerelem.

Zártláncú televíziós rendszer

Aktív kamerájú zártláncú televíziós megfigyelésről akkor beszélünk, ha a képernyőt egy kezelő figyeli, aki irányítani tudja a kamerát (elfordíthatja, ránagyíthat vele a képre), és így követni tudja az egyént vagy a kialakult helyzetet. Az aktív kamerák automatizált vizuális megfigyelőprogramokkal társíthatók, amelyek algoritmusok segítségével érzékelik a gyanús mozgást, azonosítják az embereket egy adatbázisban szereplő sablonok segítségével.

Passzív kamerák: Ezek a kamerák szalagra veszik fel, ami egy adott helyen (például egy üzletben) történik. A szalagot csak akkor nézik meg, ha baj történik, például betörés, tűzeset, stb. esetén.

Míg a korábbi zárt láncú videórendszerek analóg elven működtek, addig az utóbbi időben ezen a területen is egyre inkább teret hódít a digitális technika. A digitális képkereséssel időt takaríthatunk meg egy adott esemény visszakeresésekor, vagy ha bűnelkövetéssel gyanúsított személyeket akarunk megtalálni már létező adatbázisban. Ugyanakkor aggodalomra ad okot, hogy ezek a képek könnyebben manipulálhatók.

Automatikus arcfelismerés

Az automatikus arcfelismerő rendszer olyan rendszer, amelyben az adott személyről automatikusan felvétel készül, és ezt a felvételt összevetik egy azonosítást vagy hitelesítést szolgáló adatbázissal. Véletlenszerűen kiválasztott személy azonosítása ezzel a technikával rendkívül nagy adatbázist és olyan feldolgozási kapacitást igényelne, ami ma még nem valósítható meg. Az ilyen rendszereket így jelenleg arra használják, hogy megállapítsák, rajta van-e az adott személy például az ismert bűnözők vagy terroristák listáján.

Automatikus rendszámfelismerés (angol rövidítése: ANPR)

Az automatikus rendszámfelismerő rendszerek beolvassák a zártláncú televízió kamerái által rögzített rendszámokat, és összehasonlítják azokat egy adatbázissal. Ilyen rendszereket több országban alkalmaznak, leginkább a díjfizető kapuknál és a gyorshajtás ellenőrzésénél, de lopott járművek azonosítására is használják.

Péter nem is tudja mindegyikről, hogy mire szolgál. Az eCall rendszer manapság már az új autók alapfelszereltségéhez tartozik, s arra szolgál, hogy baleset esetén automatikusan felhívja a segélyhívó számot. Mivel kapcsolatban áll a Galileo rendszerrel, pontosan tudja, hol van az autó.

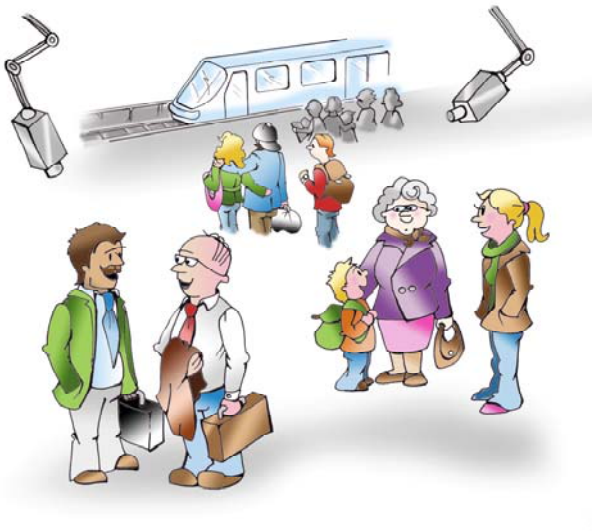
Az utóbbi években felmerült e technika másfajta alkalmazásának lehetősége is. Berlinben egy meghiúsult terrorista akció

után a terroristák elloptak egy autót, és azzal menekültek Németországon keresztül. Ekkor kiderült, hogy a rendszer arra is alkalmas, hogy a segítségével megtalálják, sőt megállítsák a kocsit. Az ellopott autó ugyanis egy drága modell volt, amit a legújabb lopás elleni technikákkal láttak el, s történetesen a műholdon keresztül, távirányítással le lehetett állítani. A terroristákat megállították és letartóztatták. Ez után az Európai Unió országai hozzájárultak ahhoz, hogy a rendszert a rendőrség is használhassa a bűnözők és a terroristagyanús személyek megtalálására.

Kutatási jelentés készült arról, hány emberéletet lehetne megmenteni a

közlekedésben, ha a járművezetők betartanák a sebességkorlátozásokat. A kutatás eredményeinek ismeretében az a javaslat született, hogy a járműbiztonsági rendszerekbe építsenek bele egy modult, ami képes lenne a sebességkorlát ellenőrzésére az adott útszakaszon, és összehasonlítaná ezt az autó sebességmérőjének az állásával. Az eredeti javaslat az volt, hogy a kocsik motorjába építsenek bele egy csipet, ami gondoskodik arról, hogy a jármű ne gyorsulhasson a megengedett sebesség fölé. Ez azonban heves ellenállást váltott ki mind az autóipar, mind az autótulajdonosok szövetségének részéről. Jelen pillanatban a rendszer úgy működik, hogy amint egy autó túllépi a megengedett sebességet, hívás megy a központi bírságnyilvántartóba, és a bírságot automatikusan levonják az autótulajdonos bankszámlájáról.

Péter gázt ad. Még nem frissítettek (vagy raktak be) minden útszakaszt a rendszerben, ezért letöltötte a navigációs rendszeréhez szükséges áttekintést. Valahányszor elhajt egy olyan jel mellett, ami hozzá van kapcsolva a rendszerhez, figyelmeztetést kap, hogy a megengedett sebességhatárt be „kell” tartania. „Jó, hogy a megfigyelőrendszer fordítva is működik” – gondolja Péter.



Péter megérkezik a reptérre. A rendszáma már szerepel a rendszerben, így a kocsija automatikusan bejelentkezik, amikor behajt a parkolóba.

Helymeghatározó

Megközelítőleg ki lehet számítani a felhasználó mobiltelefonjának helyzetét, például a GSM bázisállomások ismert koordinátáinak segítségével.

Pontosabb helymeghatározásokra műholdas rendszereket használnak.

A GPS a *Global Positioning System* (Globális Helymeghatározó Rendszer) rövidítése, ami

egy az egész világra kiterjedő műholdas navigációs rendszer. Huszonnégy Föld körül keringő műhold alkotja. Három műhold felhasználásával a GPS képes kiszámítani a fogadó (vevő) eszköz helyének földrajzi hosszúságát és szélességét a három gömb metszéspontja alapján.

A *Galileo* rendszer 30 műhold globális navigációs hálózata lesz, aminek segítségével a felhasználók a földön és a levegőben pontos idő- és helymeghatározást kaphatnak. A tervek szerint 2010-re már teljes egészében működni fog. Pontosabb lesz a GPS rendszernél, s nagyobb lesz a hatóköre is.

eCall (intelligens segélyhívó)

Az eCall segélyhívó eszköz olyan érzékelőket tartalmaz, amelyek baleset esetén működésbe lépnek. Az eszköz felhívja a segélyhívószámot, közli a segélyközponttal a balesetre vonatkozó információkat, például az idejét, a pontos helyszínét, az irányát és az autó azonosítóját.

Az eCall nem kapcsolódik folyamatosan semmilyen mobil kommunikációs rendszerre, csak a működésbe lépés (a baleset) után. Aggályok merültek fel azonban amiatt, hogy ez még változhat, valamint a járulékos adatok átkerülése (például a biztosító társaságokhoz) miatt és amiatt, hogy esetleg illetéktelenek is hozzáférhetnek azokhoz az adatbázisokhoz, amelyekben az eCall adatait tárolják. 2009 szeptemberétől a résztvevő országokban valamennyi új autót felszerelnek ezzel az intelligens segélyhívó eszközzel.

Ugyanazt a technikát alkalmazzák itt, mint a városokban a lopott járművek azonosítására. Péter véleménye szerint ez a rendszer fölöslegessé vált a Galileo rendszerhez kapcsolt eCall eszköz bevezetésével, de nyilvánvalóan a szervezettebb bandák tudták, hogyan lehet hatástalanítani a rendszert. Sőt arról is tud, hogy egyes országokban egyenesen ragaszkodnak ahhoz, hogy az autó vezetőjének lehetősége legyen arra, hogy saját maga kikapcsolhassa az eCall rendszert. Az ilyen elvárások mindig megnehezítik az autóipar helyzetét. S miért van az, hogy a bűnözők mintha mindig egy lépéssel a technika előtt járnának?

Céleltolódás

Az adatbázis-rendszerek ki vannak téve az ún. „céleltolódásnak”, vagyis annak a veszélynek, hogy az összegyűjtött adatokat nem arra használják fel, mint ami miatt összegyűjtötték őket. Ez történt például Norvégiában, amikor a menedékkérők adatbázisát – ami olyan biometrikus azonosítókat is tartalmaz, mint például az ujjlenyomat – hozzáférhetővé tették a bűnügyi nyomozók számára. Az adatbázis eredetileg azzal a céllal készült, hogy segítsen a menedékkérők személyazonosságának a létrehozásában, meghatározásában..

Leparkolja az autóját, kiszáll, elindul a terminál, azon belül is a gyors sávú bejelentkezés bejáratához. A mutatóujját ráteszi az érzékelőre, és egyenesen a kamerába néz. Zöld fény villan fel, és az ajtó kinyílik.

Bár az érzékelők már sokkal fejlettebbek, mint régebben, néhány embernek még mindig gondot okoz az ujjlenyomatvétel: Többek közt saját nagyapjának. Bár az öreg nagyon mozgékony nyolcvan éves korához képest, egyre inkább elszigetelődik. Manapság mindenütt kérik az ujjlenyomatot a személyi igazolvány mellé, s a nagyapját kényelmetlenül érinti a sok zűrzavar, amelyen keresztül kell esni, ha az érzékelő nem tudja elolvasni az ujjlenyomatunkat. Ezért legtöbbször inkább otthon marad.

Péter időnként elmegy a könyvtárba, hogy valódi könyveket kölcsönözzön. Mókásnak tartja, ha eszébe jut, hogyan nézhet ki más ember szemében saját könyvtári profilja. Ha gyanús személyek keresése közben valamikor is elemeznék, a hírszerző szolgálat emberei biztosan csodálkoznának, vajon miért kölcsönöz ki egy a harmincas éveiben járó ember olyan könyveket, mint például a „Randevúzás idősebbeknek” vagy a „Barátaink a madarak”.

Néhány évvel ezelőtt az Egyesült Államokban, közvetlenül egy nagyszabású terrorista akció leleplezése után tényleges javaslatként merült fel, hogy a biztonsági szolgálatoknak legyen joguk átvizsgálni minden rendelkezésre álló adatbázist. S ez nem pusztán a bűnöző vagy terroristagyanús személyek adatbázisára vonatkozott. Elemezni akarták a könyvtári adatbázisok teljes anyagát, a villany- és a gázfogyasztási szokásokat, a telefon- és internet-adatforgalmat, az utazási adatokat és a vásárlási szokásokat. A gyanús minták felderítésével kívánták kiszűrni a lehetséges terroristákat.

Páter munkatársa, Alex magán kívül volt a felháborodástól, s Péter igyekezett érveket felsorakoztatni Alex véleménye ellen: biztos nem kérnék ezt, ha nem lenne rá jó okuk. A hatóságoknak mindent el kell követniük, hogy elkapják a terroristákat. Alexet azonban nem lehetett meggyőzni, és szerinte legalább névtelen adatokon kellett volna elvégezniük az elemzéseket. „S ha találnak valami gyanúsat, akkor kellene engedélyt kérniük a bíróságtól a személyazonosság felfedésére. Nincs törvényes joguk ahhoz, hogy mindenkiről megtudhassanak mindent.”

Pétert nem igazán érdekelte tovább a kérdés, de a munkatársa minden ebédszünetben szóba hozta, míg a végén Péter aláírta a javaslat elleni tiltakozást. „De nem látom be igazán, hogy miért van erre szükség“ – mondta. „Nem csupán azoknak gond ez, akiknek valamilyen takargatnivalójuk van?” Másrészt viszont nem hagyta nyugodni a gondolat, vajon feljegyezték-e valahol, hogy aláírta a tiltakozást…

Teljes Információs Éberség (Total Information Awareness: TIA)

A Teljes Információs Éberség (TIA) az Egyesült Államok védelmi minisztériuma kutatási és fejlesztési ügynökségének (DARPA) egyik programja volt. A TIA program három eszközkategóriából épült fel: nyelvi fordítótechnikákból, adatkereső és mintázatfelismerő technológiákból, valamint fejlett együttműködési és döntéstámogatási eszközökből.

A TIA célja a terrorista akciók felderítése volt még a bekövetkezésük előtt. A rendszert arra tervezték, hogy a magán- és a nyilvános adatbázisok, valamint az internet megfigyelésével kiszűrjék az olyan tranzakciókat, amelyeknek közük lehet terrorista akciókhoz. Az USA kongresszusa 2003 szeptemberében beszüntette a TIA támogatását, de a rendszeren belüli programok közül sok tovább él különböző nevek alatt.

Klára a csendes zónában üldögél, és egy ideig a könyvét olvassa, majd elindul a biztonsági kapu felé.

Azért állítottak fel biztonsági kapukat a nemzetközi vasúti pályaudvarokon, mert nemcsak a repülőtereken, de más olyan helyeken is megnövekedett az ellenőrzés iránti igény, ahol sok ember gyűlik össze. Klára tudja, hogy más országokban már a bevásárlóközpontok és a stadionok bejáratánál is ellenőrzik a belépőket. Néhány évvel ezelőtt a fia lakhelyéhez közeli bevásárlóközpontnál így kaptak el egy robbantót. Úgy látszik, akkor kezdhették el a szűrőkaput alkalmazni a bejáratnál, és a robbantó még nem tudott róla. Ennek ellenére örül, hogy náluk még nem jutottak ilyen messzire a dolgok. Mindmáig csupán a repülőtereken és a pályaudvarokon ellenőrzik az utasokat.

Klára nem igazán aggódik a bevásárlóközpontok miatt, végül is amennyire tudja, az országban, ahol él, még nem volt semmi ilyen jellegű fenyegetés. Olvasott azonban olyan statisztikákat, amelyek szerint egyre többen visszatérnek vásárolni a kis- és a nagyvárosok központjában található kisebb üzletekbe, s hogy a bevásárlóközpontok azt állítják, azért veszítenek a bevételükből, mert nem állíthatnak fel olyan szűrőkapukat, amilyenek például az ún. *vetkőztetőgépek*.

Klára előveszi az útlevelét, és a szivárványhártya- (írisz) letapogatóhoz megy. Tudja, hogy egyes országokban még mindig ujjlenyomatot használnak a személyi igazolványokban és az útlevelekben, ő mégis úgy érzi, az írisz alapján biztonságosabb az azonosítás. A beolvasó összehasonlítja a szivárványhártyáját az útlevelében tárolt sablonnal. Volt idő, amikor ez aggasztotta, de a fia, aki a számítástechnikai iparban dolgozik, megnyugtatta, hogy a módszer ma már teljesen biztonságos. „Az első útlevelek titkosítása eléggé gyenge volt, – mondta – de a ma használt titkosítást egy szuperszámítógép is csak sok ezer év alatt lenne képes feltörni.” Emellett az első útlevelekben az arc, az ujjlenyomat vagy az írisz tényleges képét tárolták. Ma viszont csupán ezek sablonját, vagyis az arc, az írisz legfontosabb jellemzőinek digitális megfelelőjét. Még akkor sem lennének képesek visszaállítani az arc vagy az írisz képét, hogy megtudják, kié az útlevél, ha valahogy feltörnék a kódot.

Még arról is biztosították, hogy a beolvasó csupán annyi ideig tárolja az íriszéről előállított sablont, amíg összehasonlítja azt a kártyáján lévővel, és nem kerül be egy központi adatbázisba. Azt azonban nem tudja, mi történik akkor, amikor egy másik határon ellenőrzik az útlevelét. Ott is kitörlik az adatokat az összehasonlítás után?

Rádiófrekvenciás Azonosítás (angol rövidítése: RFID)

Az RFID rádióhullámok segítségével történő automatikus azonosítást jelent. Parányi integrált áramköröket (címkéket) erősítenek a dokumentumokra, illetve építenek bele a termékekbe. Adott távolságon belül *leolvasóeszköz* segítségével kapható meg a címkén található információ.

Az RFID címke lehet *aktív* vagy *passzív* csip. Az aktív címkék – amilyenek például a fizetős autópályák díjfizető kapujánál használt zsetonok – áramforrást tartalmaznak, így méretre nagyobbak a passzív címkéknél, viszont több információt tartalmazhatnak, és nagyobb a hatótávolságuk. A passzív címkék nem tartalmaznak áramforrást, az energiájukat

a leolvasó rádióhullám jele generálja. A passzív címkék tipikus alkalmazására jelen pillanatban az új európai útlevél a példa.

A címkék többsége hozzáférhető a legtöbb leolvasóval, de vannak olyan címkék is, amelyek jelszót vagy más azonosítót kérnek a leolvasótól.

Biometrikus útlevél

A biometrikus útlevél a tényleges dokumentumból, rendszerint kis füzetkéből, és egy parányi csipből áll.

A csip kötelező és választható adatokat tartalmaz. Emellett van benne fénykép is, ami képi kapcsolatot teremt az útlevél tulajdonosa és az útlevél között.

A Nemzetközi Polgári Légiközlekedési Szervezet (ICAO) olyan csip alkalmazása mellett döntött, ami (az RFID címkéhez hasonlóan) bizonyos távolságból leolvasható. Az ICAO az *arcot* választotta elsődleges, útlevélbe kerülő biometrikus azonosítónak. Az ujjlenyomatot és az írisz képét pedig másodlagos biometrikus azonosítónak ajánlotta. Az EU mindössze az ujjlenyomatot választotta másodlagos azonosítóként.

A biometrikus útlevél sok vitát váltott ki, különösen a biometrikus információ biztonságosságával kapcsolatban. Attól tartanak, hogy az információ ún. lefölözéssel (vagyis bizonyos távolságon belül a tulajdonos tudta nélküli leolvasással) vagy lehallgatással (átvitel közbeni elfogással) ellopható.

A fenti aggodalmaknak az eloszlatására kifejlesztették az ún. egyszerű hozzáférés-ellenőrzési (BAC) eljárást. A BAC alkalmazásakor a megfigyelőrendszer egyszerű hozzáférési „kulcsot” használ a csip „kinyitására”, hogy a rendszer el tudja olvasni. A kulcsot az eszköz az útlevél gép által leolvasható részében (vonalkód) szereplő számadatokból generálja. A BAC-t kritikusai nem ítélik elég biztonságosnak, s biztonsági szakértők rövid idő alatt fel tudták törni a titkosítás kódját.

Néhány éve botrány tört ki egy központi ujjlenyomat-adatbázis körül, ha Klára jól emlékszik, az Egyesült Államokban. Az egyik alkalmazott ellopott egy halom ujjlenyomatot, és eladta őket nemzetközi bűnözőknek. Sok ezer ember személyi azonosítóját lopták el, akiknek emiatt mindenféle gondjuk támadt: „feketelistán” találták magukat például a

határállomásokon, vagy éppen kiürítették a bankszámlájukat. Különösen nehéz helyzetbe kerültek, mivel a kormány csak igen hosszú idő után ismerte el az adatok elvesztését. Időközben pedig senki nem hitte el nekik, hogy ellopták a személyi adataikat, vagy hogy egyáltalán lehetséges lett volna valaki más ujjlenyomatát felhasználni személyazonossága ellopására!

Klára azonban mást is tudott erről. Múlt nyáron fia egyik barátjának ellopták a személyi igazolványát, éppen mielőtt nyaralni indult volna a családjával. Félt, hogy törölniük kell az egész nyaralást, mert „feketelistára" teszik, de úgy látszik, a schengeni információs rendszer (SIS), amit sok európai országban használnak, nyilvántartja azokat, akiknek ellopták a személyes iratait. Így gond nélkül elutazhatott a családjával, sehol senki nem gyanúsította azzal, hogy bűnöző vagy terrorista lenne, bár a személyazonosságát valószínűleg alaposabban ellenőrizték, mint az átlagos utazóét.

A személyazonosítás után Klárának át kellett küldenie a bőröndjét a csomagvizsgáló röntgenberendezésen, mielőtt maga átment a régebben csak „vetkőztetőgépnek" nevezett kapun. Klára örül, hogy az igazi vetkőztetőgépet soha nem állították fel hazája repülőterein és nemzetközi pályaudvarain. A biztonsági hatóságok többféle gépet megvizsgáltak, de úgy döntöttek, hogy ugyanolyan biztonságos az a berendezés, ami a rejtett tárgyakat egy semleges emberi sablonalak képére vetítve jeleníti meg.

Utasvizsgálat (*„vetkőztetőgépek"*)

A *visszaverődő röntgenhullámok* vagy az *ultramikrohullámú sugárzás* az optikai sugárzásnál mélyebben hatol az anyagba. Ez azt jelenti, hogy mindkettő felhasználható a ruházat alatt elrejtett tárgyak érzékelésére.

Az ún. „vetkőztetőgép" ilyen technika segítségével mutatja meg, ha valaki testére erősített fegyvert vagy robbanószert visz. Többféle rendszer van, vannak olyanok, amelyek nemcsak lőfegyvereket és robbanószereket, hanem mindent megmutatnak a ruházat alatt. Innen származik az elnevezés is. Ilyen típusú reptéri biztonsági berendezés működik 2004 óta a Heathrow repülőtér 4-es terminálján. Más alkalmazások csak az elrejtett tárgyakat mutatják meg egy semleges emberi alakra vetítve.

Klára még 62 évesen is feszélyezve érzi magát a meztelenséggel kapcsolatban, ezért örül, hogy a biztonsági kapunál szolgálatot teljesítő fiatalember nem látja őt meztelenül. Le kell vennie a cipőjét, de ettől eltekintve más kellemetlenséget nem tapasztal, s nemsokára kényelmesen elhelyezkedik a vonaton.

- o -

Péter átvág a várótermen a biztonsági ellenőrzés felé. Természetesen a gyors sávra bejelentkezett utasoknak is át kell esniük bizonyos biztonsági ellenőrzésen, de saját kapujuk van, és mindannyian jól tudják, mi vár rájuk. Ennél a kapunál senki nem visel fémcsatos övet, és nem hagy aprópénzt amatőr módon a zsebében. S az üzletemberek számára készült cipők már évek óta nem tartalmaznak fémet. Behúzza a hasát, és átsétál a vetkőztetőgépen. „Miért van ebben a szobában mindig ilyen hideg" – gondolja, és elpirul, amikor látja, hogy az egyik biztonsági őr megközelítőleg saját korabeli nő. Ennek ellenére örül, hogy a repülőtér az igazi vetkőztetőgépet alkalmazza. Valahogy biztonságosabbnak érzi.

Adatmegőrzés

Az adatbázis definíció szerint adatok rendezett gyűjteményét jelenti. Széles körben elismert, hogy az egymással összekapcsolt adatok többet elárulnak a személyről, akire vonatkoznak, mint külön-külön. Éppen ezért fontos személyes adatvédelmi elv, hogy olyan adatbázisokba, amelyek személyekre vonatkozó információt tartalmaznak, kizárólag olyan adatok gyűjthetők, amelyek szükségesek a rendszer célja szempontjából, s amikor már nincs többé szükség rájuk, ki kell őket törölni.

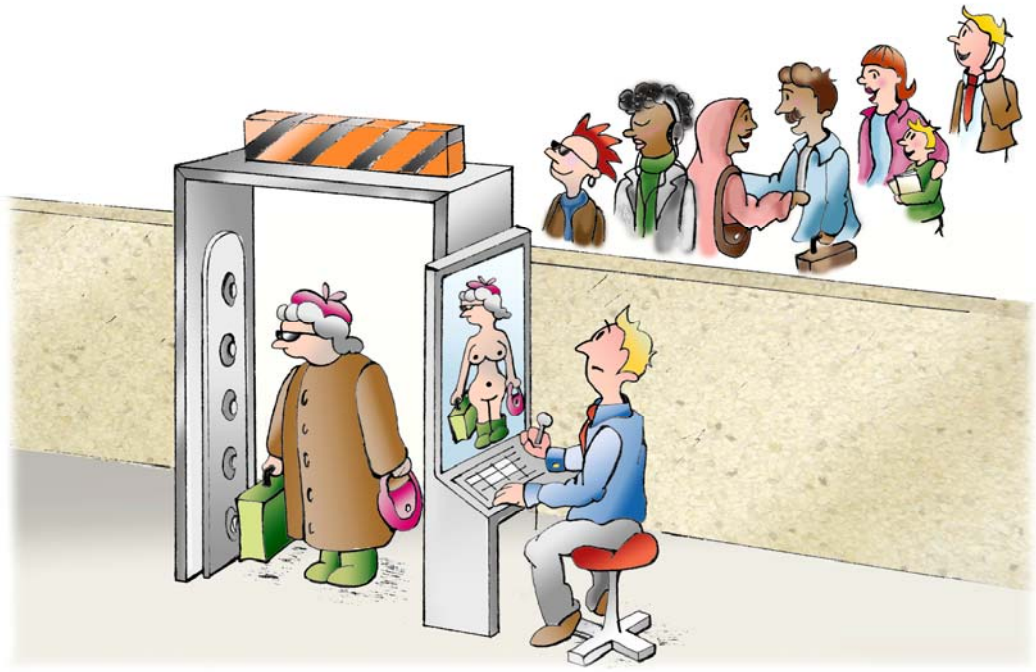
Az utóbbi időben azonban az a tendencia, hogy a kormányok több adatot szeretnének tárolni, és össze akarják vonni a különböző adatbázisrendszereket az eredetitől eltérő céllal, például a terrorizmus elleni küzdelem érdekében. Az adatmegőrzéssel kapcsolatban rendszerint az információtechnológiához kapcsolódó adattípusok kerülnek szóba, például a telefonon, a mobiltelefonon és az internetforgalomban megszerezhető kommunikációs adatok.

Az EU irányelvet fogadott el az ilyen típusú adatok megőrzésére vonatkozóan. Ez alapján megőrzik, eltárolják azokat az adatokat, amelyek elárulják, hogy ki, mikor és hol kommunikált, de a közlés tartalma nem. Az adatok legfeljebb két évig őrizhetők meg.

A jelentések szerint különböző amerikai minisztériumok 2005-ben megközelítőleg 30 millió dollárért vásároltak személyes adatokat ún. *információs viszonteladóktól*. Ezek a vállalkozások különféle forrásokból gyűjtik és halmozzák fel a személyi adatokat, amelyeket aztán eladnak vásárlóiknak. A források lehetnek nyilvános adattárak, nyilvánosan (például az interneten) hozzáférhető információk, és védett források, például magánvállalkozásoktól.

Péter észreveszi, hogy új biztonsági berendezés van a megszokottak mellett, amelyet eddig még nem látott. A vetkőztetőgép után egy másik „kapu” is áll, és az utasok egy részét megkérik, hogy menjenek át rajta. Halványan emlékszik, hogy hallott valamit egy új biztonsági eszközről, amelyet ezen a reptéren próbálnak ki. Állítólag olyan jellemzőket rögzít, mint a testhőmérséklet, az izzadás mértéke, a szívverés,. tehát olyan dolgokat, amelyek betegségek – például atípusos tüdőgyulladás (SARS), madárinfluenza – tünetei lehetnek vagy a vizsgált személy idegességét jelezhetik. A kapun átlépők egy részét a közeli kikérdezőszobába kísérik. Bár Péter egészséges és tiszta a lelkiismerete, mégis örül, hogy nem választották ki tesztalanynak. „De miért éppen a gyors sávra tették ezt a berendezést? Nem tudják, hogy azok, akik ezt választják, sietnek?”

A beszállókapuhoz megy, és helyet foglal. Nem kellene felhívnia Yasmint, hogy



megmondja, jön? Yasmin annak az autógyártó cégnek dolgozik, amelyet Péter autókereskedése képvisel, és a legutóbbi autó-bemutatón találkoztak. Azonnal megértették egymást, s Péter alig várja, hogy újra találkozzanak. Másrészt viszont nem szívesen hívja fel a mobilján. Tudja, hogy Yasmin bátyja igen aktív tagja mecsetje ifjúsági csoportjának, s ezért Yasmin valószínűleg szerepel valamilyen megfigyelési listán, mint a bátyja „hálózatához" tartozó személy. Arra gondol, bárcsak vásárolt volna néhány névtelen telefonkártyát, amikor legutóbb Ázsiában járt. Európában törvényesen már nem lehet ilyeneket árusítani.

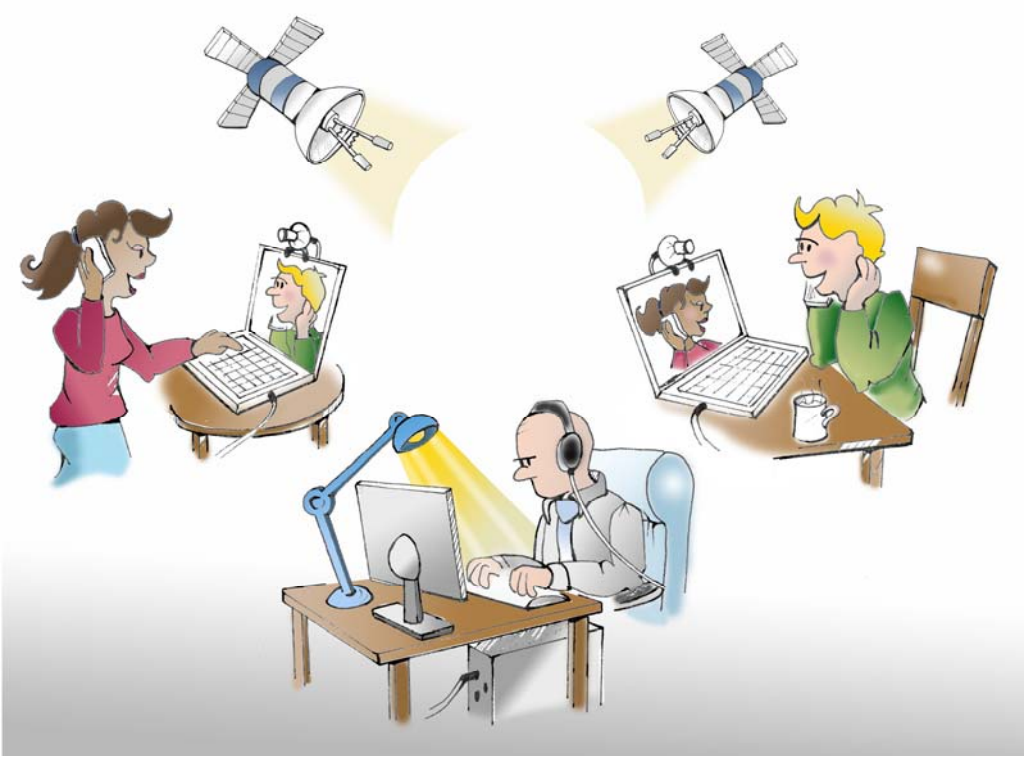
Lehallgatás

Az állampolgárok és a közöttük folytatott kommunikáció megfigyelése különböző módszerekkel lehetséges mind az interneten, mind a telefonvonalakon keresztül, mind pedig meghatározott helyeken. Az illetéktelen lehallgatás egyik formáját gyakran emlegetik *vezetékmegcsapolás* néven. Ez a gyakorlatban azt jelenti, hogy lehallgató eszközt szerelnek a két telefon közé, amelyen a beszélgetés folyik. A vezetékmegcsapolás beépíthető a gyanús személy vagy azon személyek telefonjába, akikkel várhatóan kapcsolatot létesít.

A vezetékmegcsapolás kiterjesztett módozata, amikor minden megkülönböztetés nélkül valamennyi kommunikációs vonalat (telefon, mobil, internet) lehallgatnak érdeklődésre számot tartó beszélgetéseket keresve. Példa erre az Echelon hálózat, amit az USA, Nagy-Britannia, Kanada, Ausztrália és Új-Zéland közösen működtet. A rendszert eredetileg a Szovjetunión és Kelet-Európán belüli, illetve az oda irányuló kommunikáció megfigyelésére állították fel. Segítségével elemezhetők a kommunikációs minták, és bizonyos kulcsszavak alapján a tartalom is szűrhető.

Interneten sem szeretne kapcsolatba lépni vele. Ki tudja, mi mindent naplóz a reptéri hálózat. Még abban sem biztos, milyen szabályok vannak érvényben manapság. Vajon a rendőrség közvetlenül hozzáférhet az ilyen adatokhoz vagy csak engedéllyel? Hirtelen azt kívánta, bárcsak nagyobb figyelmet szentelt volna a személyes adatok védelméről folyó vitának. Elhatározta, hogy megkérdezi erről a munkatársát, amint a gépen lesznek.

Legutóbb, amikor együtt vacsoráztak, Yasmin említette neki, hogy biztosan tudja, hogy figyelik az e-mailjét, s arra kérte,



használjon titkosító programot, amikor neki ír. „A titkosítás nélküli e-mail olyan, mint egy képeslap – magyarázta. – Tudtad, hogy bárki elolvashatja, aki hozzáfér?”

Tényleg akart is neki írni, de felfedezte, hogy a munkahelyén használt levelezőprogramban nem volt lehetőség a titkosításra, arra pedig soha nem jutott ideje, hogy másik programot telepítsen a gépére. Reméli, Yasmin nem haragszik rá, amiért ilyen hosszú ideig nem kereste. „Majd elmondom neki, mi történt, ha találkozunk” – gondolja.

Elérkezett a beszállás ideje. A beléptető kapuhoz megy, ráteszi mutatóujját az érzékelőre, s az első utasok között száll fel a gépre. Még bőven van hely a kézipoggyászok számára. A munkatársára gondol, aki bizonyára még mindig sorban áll a biztonsági ellenőrzésre várva, majd hátradőlve lecsukja a szemét.

- o -

– Mama már úton van – mondja Klára fia a feleségének, miután üzenetet kapott a mobilján. – Három órán belül ide kell érnie. Az anyja nem tudja, de az új mobil, amit karácsonyra kapott tőle, kapcsolatban áll az ún. gyerek-figyelő rendszerrel. Ez a technika a régi kémfilmekből ismert nyomkövetők modern változata, amelynek segítségével a megfigyelő apró pontként követheti a gyanúsítottat egy térképen. A legnagyobb különbség a régi és az új között, hogy a mobilba épített Galileo-technika segítségével akkor is követheti anyja mozgását egy térképen, ha Klára történetesen saját nappalijában üldögél egy másik országban.

Magánszféra-védő technológiák (angol rövidítése: PET)

A közvetlenül a személyes adatok, a magánszféra védelmét célzó technológiákat magánszféra-védő technológiáknak nevezzük (Privacy enhancing technologies: PET).

Az egyik *anonimitást* (névtelenséget) biztosító technológia a PET. Léteznek olyan szolgáltatások, amelyek lehetővé teszik a névtelen elektronikus kommunikációt a rendszeres felhasználók számára. Ezek a technikák elrejtik a kapcsolatot a felhasználó és a maga mögött hagyott nyomok között, így elkerülhetővé válik a nemkívánatos azonosítás. A hagyományos készpénzes fizetés és a nem-regisztrált (anonim) telefonkártyák olyan eszközök, amelyek lehetővé teszik az anonimitást (azonosíthatatlanságot).

Az *azonosítás-kezelés* ugyancsak a PET egyik formája. Vannak esetek, amikor nem szeretnénk azonosítani magunkat, inkább álnevet használunk (például internetes fórumokon). Az adatok megfeleltetésének megnehezítése érdekében jó, ha különböző célokra más-más felhasználói nevünk (amelyek nem fedik fel a kilétünket) és jelszavunk van. Az azonosítás-kezelő rendszerek abban segítenek bennünket, hogy el tudjunk igazodni különböző felhasználói neveink között. Az esetek egy részében a szóban forgó szolgáltatás csupán valamilyen speciális jellemző – például az életkor vagy a hitelkeret – igazolását kéri. Ilyen esetekben az *identitásnyújtó* (pl. a bankunk, a telefoncégünk vagy a munkáltatónk) megbízható harmadik félként szerepelhet, és garantálhatja a kért jellemzőt identitásunk felfedése nélkül.

A titkosítás a tartalom olyan módon való torzítására szolgál, hogy az mások számára olvashatatlan legyen. Mivel minden elektronikus úton zajló kommunikáció ki van téve a lehallgatás vagy a manipuláció veszélyének, sok esetben létfontosságú, hogy a kommunikációs csatorna vagy maga a tartalom (az üzenet) titkosított legyen.

Igyekszik azonban, hogy ne kelljen túl sokszor használnia, mert nagyon is olyan érzés számára, mintha anyja magánélete után leskelődne, de beállított néhány olyan eshetőséget, amelynek bekövetkezésére a mobilja hangjelzést ad. Ilyen például, ha az anyja sokáig nem mozog a házában vagy ha éjjel nincs otthon. Végül is egyre idősebb, és mivel másik országban él, nem tud úgy vigyázni rá, ahogy szeretne. Megszólal a telefonja: „Szia, itt Anyu! Már úton vagyok, s ha minden rendben, körülbelül három óra múlva ott leszek az állomáson…”