

Sorveglianza, privacy e sicurezza

QUAL È LA TUA OPINIONE?

surprise
surveillance
privacy
security



Questo progetto è finanziato dal Settimo Programma Quadro di ricerca dell'Unione Europea in base all'accordo di assegnazione numero 285492.

Indice

1	Benvenuti a SurPRISE	5
2	Riepilogo	6
3	Sorveglianza, privacy e sicurezza	8
3.1	Sorveglianza	8
3.2	Privacy e protezione dei dati: questioni importanti?	8
3.3	Sicurezza	9
4	Cinque tecnologie per la sicurezza	11
5	TVCC smart	12
5.1	Perché è stata messa a punto la TVCC smart	12
5.2	Come viene usata la TVCC smart	13
5.3	Miglioramenti relativi alla sicurezza	14
5.4	Problematiche	14
6	Droni	16
6.1	Perché sono stati realizzati i droni	16
6.2	Come vengono usati i droni	17
6.3	Miglioramenti della sicurezza	18
6.4	Problematiche	18
7	Cybersorveglianza mediante Deep Packet Inspection (DPI)	20
7.1	Perché è stato messo a punto il DPI	21
7.2	Come viene usato il DPI	21
7.2.1	Usi commerciali	22
7.2.2	Impieghi per la sicurezza pubblica e nazionale	22
7.3	Miglioramenti della sicurezza	22
7.4	Problematiche	23
8	Geolocalizzazione degli smartphone	24
8.1	Perché è stata sviluppata la geolocalizzazione degli smartphone	24
8.2	Come viene usata la geolocalizzazione degli smartphone	26
8.2.1	Usi commerciali	26
8.2.2	Impieghi per la sicurezza pubblica e nazionale	26
8.3	Miglioramenti della sicurezza	26
8.4	Problematiche	27
9	Biometria	28
9.1	Perché è stata sviluppata la biometria	28
9.2	Come viene usata la biometria	28
9.3	Miglioramenti della sicurezza	30
9.4	Problematiche	30
10	La tecnologia basata sulla sorveglianza è l'unica risposta?	32
10.1	Misure di sicurezza alternative: il livello globale	32
10.2	Misure di sicurezza alternative: il livello locale	33
11	Ora tocca a Lei	35
	Questo documento	36
	Partners di progetto	37

1 Benvenuti a SurPRISE

Benvenuti a SurPRISE - Sorveglianza, Privacy e Sicurezza: uno studio partecipativo dei criteri e fattori che determinano l'accettabilità e l'accettazione delle tecnologie di sicurezza in Europa - un progetto di ricerca a livello europeo. SurPRISE è l'acronimo di "Surveillance, Privacy and Security: Sorveglianza, privacy e sicurezza". Il suo obiettivo è quello di raccogliere i pareri dei cittadini sulle nuove tecnologie per la sicurezza. Molte di queste tecnologie si basano sulla sorveglianza delle persone e delle loro azioni. Vengono utilizzate dalla polizia o da agenzie di vigilanza per monitorare ciò che sta avvenendo, per scoprire e prevenire problemi di sicurezza. Quando Lei va in aeroporto e il Suo bagaglio viene controllato dagli appositi scanner, oppure quando un impianto di videosorveglianza registra gli spostamenti su una strada in cui Lei sta camminando, Lei entra in contatto con le tecnologie per la sicurezza basate sulla sorveglianza. Lo scopo di SurPRISE è di garantire che queste tecnologie siano efficaci, sicure e rispettose dei diritti umani. Per raggiungere tale obiettivo, SurPRISE ha bisogno del Suo aiuto.

L'abbiamo invitata a partecipare al progetto SurPRISE perché la Commissione Europea desidera chiedere ai cittadini che cosa pensano debba esse-

re fatto per garantire la loro sicurezza. Partecipando al focus group SurPRISE Lei potrà condividere il suo punto di vista sulle nuove tecnologie per la sicurezza con altri cittadini.

SurPRISE raccoglie i pareri dei cittadini su queste nuove tecnologie in nove paesi europei: Austria, Danimarca, Germania, Gran Bretagna, Italia, Norvegia, Spagna, Svizzera e Ungheria.

Questo opuscolo fornisce informazioni di base sui temi che verranno discussi durante il focus group SurPRISE italiano a giugno 2014. Si tratta di informazioni sulle nuove tecnologie per la sicurezza che sono oggetto di studio nel progetto SurPRISE. Fornisce inoltre ulteriori informazioni su sorveglianza, sicurezza e privacy in Europa.

La Sua partecipazione al focus group è importante proprio perché Lei non è un esperto. Le abbiamo chiesto di partecipare in quanto cittadino sulla cui vita quotidiana si ripercuotono le decisioni prese dai politici europei e nazionali.

I politici stabiliscono le politiche in tema di sicurezza, ma Lei, come cittadino, deve convivere con le conseguenze di tali decisioni. Ciò rende importante la Sua opinione.

La scienza ci informa, ma non ci dice che cosa fare. La scelta è nostra: dica la Sua!

2 Riepilogo

Moltissima gente non riuscirebbe a immaginare la propria vita senza smartphone, carte di debito o Internet. Quello di cui spesso la maggior parte delle persone non si rende conto, però, è che queste tecnologie generano diversi tipi di tracce elettroniche. Queste registrazioni sono in grado di indicare dove ci troviamo nello spazio e nel tempo e talvolta anche che cosa stiamo facendo. Ad esempio le operazioni bancarie, comprese quelle fatte con una carta di debito, sono in grado di indicare il tipo di acquisti che facciamo e dove. Questi dati vengono conservati nei database delle banche e possiamo vederli sui nostri estratti conto.

Le prenotazioni aeree sono in grado di indicare se stiamo andando o tornando da una parte del mondo pericolosa. I dati del cellulare indicano la nostra posizione, a chi stiamo parlando e quanto spesso lo facciamo. Queste informazioni vengono conservate dai fornitori di servizi telefonici e Internet nelle loro banche dati. Le normative europee stabiliscono che questi dati debbano essere conservati da un minimo di sei mesi fino a un massimo di due anni. È quindi possibile individuare, rintracciare e seguire la maggior parte delle persone in vari momenti della loro vita.

Tecnologie come quelle esaminate sopra, e i dati da esse raccolti, possono offrire vantaggi a noi e anche ad altri. Dopo i gravissimi attacchi terroristici avvenuti in Europa e altrove, i governi hanno investito in tecnologie avanzate per la sicurezza che utilizzano dati personali. Hanno anche emendato leggi esistenti e ne hanno approvate di nuove per consentire l'accesso a queste informazioni a fini di sicurezza. Anche se esistono molte fonti di *intelligence* 'ufficiali', i governi si sono resi conto che le attività di probabili criminali e terroristi potrebbero essere scoperte in altri modi. Come la maggior parte dei cittadini, i criminali e i terroristi hanno conti correnti bancari, possiedono documenti di identità nazionali, usano Internet e hanno telefoni cellulari. Utilizzano inoltre sistemi di trasporto, spazi pubblici e consumano merci e servizi. Forse una maggiore conoscenza di queste attività fornirebbe la chiave per trovare criminali e terroristi. Molti governi ritengono che l'uso delle nuove tec-

nologie per la sicurezza non solo permetta di fermare chi vuol fare del male, ma anche di individuarlo prima che lo compia effettivamente. Poiché le tecnologie utilizzano le informazioni in questo modo, il progetto SurPRISE le definisce "tecnologie per la sicurezza orientate alla sorveglianza".

Una tecnologia per la sicurezza orientata alla sorveglianza è:

una tecnologia che utilizza informazioni raccolte in vari contesti e relative alla popolazione e alle sue attività allo scopo di affrontare un problema riguardante la sicurezza.

Queste tecnologie analizzano le informazioni generate dai cittadini nella loro vita quotidiana. Utilizzano informazioni provenienti, ad esempio, dai cellulari, da Internet e da tecnologie *smart* come gli impianti di videosorveglianza digitali, per cercare di identificare criminali e terroristi, talvolta prima che entrino in azione.

In questo opuscolo esamineremo approfonditamente cinque di queste tecnologie:

- **TVCC smart:** impianti di videosorveglianza a circuito chiuso che vanno al di là del semplice monitoraggio degli spazi pubblici. La TVCC smart è caratterizzata da telecamere digitali collegate tra loro in un sistema che è in grado di riconoscere i volti delle persone, analizzare i loro comportamenti e individuare oggetti.
- **Droni civili:** i droni civili sono aereomobili senza pilota a bordo (UAV) per uso non militare. Possono essere utilizzati per un'ampia gamma di attività di sorveglianza. Un drone può essere equipaggiato con una telecamera e con tecnologie a sensore aggiuntive, e i droni possono essere considerati come versioni mobili delle videocamere a circuito chiuso.
- **Cybersorveglianza tramite Deep Packet Inspection (DPI)** (filtraggio dei pacchetti di dati che transitano sul web): usando dispositivi hardware e un software specifico è possibile leggere, analizzare e modificare tutti i messaggi e le informazioni trasmessi su Internet.
- **Geolocalizzazione degli smartphone:** analizzando i dati di posizione provenienti da un cel-

lulare è possibile raccogliere informazioni sulla localizzazione e sui movimenti dell'utente telefonico in un determinato arco di tempo. La posizione del cellulare può essere individuata utilizzando dati provenienti dalle antenne al quale si è connesso oppure – con maggiore precisione – mediante sistemi satellitari di posizionamento globale (GPS) o dati wireless.

- **Biometria:** la biometria si riferisce a metodi automatizzati di riconoscimento basati sulla misurazione delle caratteristiche fisiche o comportamentali degli individui. L'uso più comune della biometria è il passaporto biometrico basato sul riconoscimento facciale, delle impronte digitali e/o dell'iride.

Ciascuna di queste tecnologie è in grado di migliorare la sicurezza, identificando i sospetti e le attività criminali o illegali. Alcuni ritengono che possano anche rendere la vita molto più comoda. Ma ognuna di esse presenta una serie di svantaggi. La TVCC smart, così come i droni civili dotati di telecamera, ad esempio, funzionano solo in determinate condizioni e possono generare molti falsi allarmi. La Cybersorveglianza tramite DPI compromette la riservatezza delle comunicazioni on-line. La geolocalizzazione degli smartphone è difficile da controllare, perché molte app trasmettono dati di localizzazione dal cellulare a insaputa dell'utente. La fuga di informazioni da banche di dati biometrici potrebbe provocare furti d'identità. Il mancato controllo sulla raccolta e sull'utilizzo delle informazioni è una questione legata a tutte le tecnologie oggetto del nostro esame.

L'uso di queste tecnologie solleva questioni relative a diritti umani, privacy, regolamentazione e fiducia. Di solito queste tecnologie raccolgono e condividono dati relativi a una persona a insaputa di quest'ultima. Vengono inevitabilmente catturati e analizzati dati relativi a persone innocenti, e nel caso di alcune tecnologie, ciò viene fatto deliberatamente. Esse hanno le potenzialità per invadere la privacy, che è un diritto fondamentale tutelato in Europa. Può anche avvenire che persone innocenti

vengano erroneamente identificate come malviventi, con gravi conseguenze per la loro vita.

Malgrado i potenziali miglioramenti della sicurezza offerti da queste tecnologie, alcuni cittadini non sono certi che l'utilizzo dei loro dati a fini di sicurezza sia una cosa positiva. Se il risultato è che tutti sono più sicuri, forse può essere accettabile. Se, tuttavia, vengono infranti diritti fondamentali, forse non potrà mai essere accettabile. Le opinioni delle persone potrebbero differire anche a seconda di ciò che pensano su tutta una serie di altre questioni, come ad esempio:

- Le tecnologie funzionano effettivamente?
- Quanto sono intrusive?
- Esiste una regolamentazione giuridica sufficientemente efficace?
- Le tecnologie vengono utilizzate nel rispetto della legislazione esistente?
- Possiamo fidarci dell'uso che ne fanno le istituzioni?
- Le istituzioni che utilizzano i dati sono sottoposte a regolamenti efficaci?
- Le istituzioni sono trasparenti e rendono conto del loro operato in caso di violazioni del diritto alla privacy in nome della sicurezza?
- Chi sorveglia i sorveglianti?
- Quali sono le alternative, e sono praticabili?

Queste sono alcune delle questioni che discuteremo durante il focus group.

Istruzione scientifica, educazione dei consumatori e soprattutto dibattiti pubblici su scienza e tecnologia sono sicuramente strumenti importanti per permettere ai cittadini di partecipare ai dibattiti ed esercitare i diritti democratici.

Nei prossimi paragrafi presenteremo alcuni termini e definizioni chiave prima di descrivere in modo approfondito le cinque tecnologie per la sicurezza che abbiamo selezionato.

Continui a leggere per maggiori dettagli su questi temi.

3 Sorveglianza, privacy e sicurezza

3.1 Sorveglianza

Quando si pensa alla "sorveglianza", probabilmente vengono subito in mente alcune immagini: si potrebbe ad esempio pensare al "Grande Fratello", sia il reality televisivo sia il personaggio del romanzo *1984* di George Orwell. Lei potrebbe quindi associare la sorveglianza alla sgradevole sensazione di essere osservato da un'organizzazione o da una persona potente ma sconosciuta.

In SurPRISE, "sorveglianza" significa 'monitorare le persone allo scopo di regolare o governare il loro comportamento' e può essere effettuata per scopi diversi. Potrebbe trattarsi di scopi di sicurezza. La polizia, ad esempio, potrebbe usare gli impianti di videosorveglianza, o droni dotati di telecamere, per individuare i malviventi in strada. La sorveglianza può avere anche scopi commerciali. Il gestore di un motore di ricerca, ad esempio, può analizzare il comportamento di navigazione utilizzando metodi di sorveglianza Internet allo scopo di migliorare il funzionamento di tale motore. La sorveglianza può essere usata per prevenire i reati e catturare i criminali, ma anche per fornire prodotti e servizi alle persone.

Se la sorveglianza è un aspetto normale della società, Lei potrebbe benissimo chiedersi che cosa c'è di sbagliato in essa. I resoconti giornalistici sulla "società della sorveglianza" sembrano sempre avere un risvolto sinistro. Il punto è che controllare una tecnologia per la sorveglianza conferisce grande potere. È importante che chi occupa tali posizioni - come forze dell'ordine, broker di dati o rivenditori di dati - detenga tale potere in modo equo e con il dovuto rispetto nei confronti delle libertà civili e della legge.

Pensare di non avere niente da nascondere o niente da temere dipende in realtà da chi La sta sorvegliando, dal perché La sta sorvegliando e da come percepisce le Sue azioni. Se Lei non ha controllo né voce in tale processo e le regole improvvisamente cambiano a Suo sfavore - a causa della Sua etnia, religione, orientamento sessuale, genere od opinioni politiche - che cosa può fare? Ecco perché

una sorveglianza eccessiva può avere un impatto negativo su altri diritti umani come la libertà di espressione. In questi casi la sorveglianza può anche minare il livello di fiducia sociale, perché la gente ha paura di essere se stessa. Nel contesto della sicurezza deve essere ponderato anche l'uso di forme diverse di sorveglianza.

3.2 Privacy e protezione dei dati: questioni importanti?

Una delle questioni principali è la privacy, e come mettere in sicurezza i dati generati e usati dalle nuove tecnologie per la sicurezza. Anche se il termine privacy può significare cose diverse per persone diverse, essa costituisce una parte importante della vita di tutti i giorni. Sono numerose le cose che Lei potrebbe voler mantenere riservate in momenti diversi:

- ciò che sta facendo, i Suoi pensieri e le Sue sensazioni;
- informazioni sulle Sue relazioni intime, sul luogo in cui si trova, sul contenuto delle Sue comunicazioni con altri per posta o e-mail, sulle Sue caratteristiche personali e sulla Sua immagine.
- Il Suo corpo: quanta parte di esso Lei rivela, se Lei è in grado di proteggerlo da contatti o indagini corporei indesiderati e il Suo controllo sull'accesso, da parte di altri, a Suoi materiali corporei come il DNA o le impronte digitali.

Pensi solo a questo: sarebbe felice se una compagnia di assicurazioni sulla vita avesse accesso illimitato ai Suoi dati medici? Oppure se la polizia potesse ascoltare tutte le Sue telefonate? Ha le tende in casa Sua? Se risponde no alle prime domande e sì alla terza, allora Lei si preoccupa ancora della Sua privacy! Non è il solo. Studi sui giovani che usano i social network hanno dimostrato che, a causa delle loro preoccupazioni per la privacy, rivelano solo dati personali molto selezionati. La gente desidera ancora condividere le informazioni, ma vuole farlo entro confini stabiliti. Per l'individuo, tutto ciò che va al di là di questi limiti rappresenta quell'ambito della vita che si desidera tenere fuori da interferenze esterne: la vita privata.

In SurPRISE definiamo la privacy come:

la capacità di un individuo di essere lasciato solo, lontano dagli occhi del pubblico, in possesso del pieno controllo sulle informazioni che lo riguardano.

Nell'Unione Europea il diritto alla riservatezza (privacy) e il diritto alla protezione dei dati personali costituiscono due diritti fondamentali. Tutti hanno bisogno del diritto alla privacy: per essere liberi di agire, incontrarsi e discutere in una società democratica. Le persone non possono esercitare le libertà democratiche se si sa tutto dei loro pensieri, delle loro intenzioni e delle loro azioni.

Le nuove leggi europee sulla protezione dei dati insistono sempre di più sul fatto che la privacy deve essere 'progettata nelle' nuove tecnologie, in modo che esse siano meno invasive della privacy fin dall'inizio. Le aziende che producono nuove tecnologie vengono incoraggiate a tener conto della privacy in ogni fase del processo produttivo. Questo nuovo approccio viene chiamato *privacy by design*, cioè tener conto della privacy sin dalla fase di progettazione.

3.3 Sicurezza

Nel progetto SurPRISE definiamo la sicurezza come:

la condizione di essere protetti contro il pericolo o di non essere esposti ad esso; una sensazione di sicurezza oppure di libertà dal pericolo o di assenza di pericolo.

La sicurezza si riferisce non solo alla protezione di oggetti fisici, come edifici, sistemi informatici, confini nazionali e così via; si riferisce anche al senso di sicurezza. In un mondo ideale, misure di sicurezza efficaci aumenterebbero la sensazione di sicurezza, ma questo non sempre avviene.

Sembra strano, ma le nuove tecnologie per la sicurezza potrebbero – visto che possono compromettere la privacy - finire per farci sentire *meno* sicuri anziché *più* sicuri. Ma ciò potrebbe non essere vero per tutti. Come nel caso della privacy, sicurezza significa cose molto diverse per persone diverse. Ciascuno di noi ha le proprie percezioni su ciò che

considera una minaccia per la sicurezza e su ciò che sarebbe disposto a fare per proteggere le cose che sono importanti per lui.

Questo è vero anche per coloro che governano la sicurezza. Essi hanno bisogno di individuare e affrontare le minacce più importanti. Ogni governo ha risorse economiche, umane e tecniche limitate da destinare alla sicurezza, per cui è necessario fare delle scelte. Per l'Unione Europea le priorità principali nel campo della sicurezza sono queste:

- aumentare la sicurezza informatica per cittadini e aziende della UE;
- scardinare le reti criminali internazionali;
- prevenire il terrorismo;
- aumentare la capacità dell'Europa di riprendersi da ogni genere di crisi o calamità naturali.

Poiché l'Europa ha deciso di concentrarsi sulla ripresa dopo ogni genere di crisi o calamità naturale, la sicurezza va ora al di là della prevenzione della criminalità e del terrorismo. L'Europa si occupa anche delle minacce all'ambiente, alle risorse naturali, alle infrastrutture, all'attività economica e alla sanità. Per i politici la sicurezza si è estesa a quasi tutti i settori della vita pubblica. Questo approccio è stato adottato da molti stati europei. Ma sarà possibile garantire effettivamente la sicurezza in tutti questi settori? Attualmente l'industria della sicurezza è un settore importante che si sta sviluppando in Europa per rispondere a tale esigenza. È rappresentata da grandi aziende nel ramo della difesa e anche da molte altre società più piccole. Gli sviluppi recenti nelle tecnologie per la sicurezza orientate alla sorveglianza sono i seguenti:

- TVCC smart, cioè impianti di videosorveglianza a circuito chiuso 'intelligenti', incentrati sulla ricerca di criminali noti e sull'individuazione di comportamenti sospetti;
- cybersorveglianza, che cerca di prevenire i danni causati da virus, hacker o ladri di identità;
- dispositivi biometrici, utilizzati per evitare che individui indesiderati entrino nel territorio e per velocizzare il transito delle persone note al governo come "viaggiatori di cui ci si può fidare";

- droni per sorveglianza aerea, in grado di spiare dall'alto attività pericolose che non potrebbero essere viste da terra. Questi dati possono essere usati per indirizzare il personale di sicurezza verso i punti in cui stanno nascendo disordini;
- sistemi informatici d'avanguardia relativi ai passeggeri, che cercano di scoprire individui potenzialmente pericolosi prima che inizino il viaggio;
- tecnologie di geolocalizzazione, che cercano di ridurre al minimo il danno alle cose in movimento e di localizzare i sospetti nello spazio fisico.

4 Cinque tecnologie per la sicurezza

Le cinque tecnologie per la sicurezza che il progetto SurPRISE sta esaminando sono le seguenti:

- TVCC smart
- Droni civili
- Cybersorveglianza tramite DPI
- Geolocalizzazione degli smartphone
- Biometria

Queste tecnologie per la sicurezza sono ancora in fase di sviluppo ed è ancora possibile stabilire una politica in merito al loro utilizzo.

Nei capitoli seguenti di questo opuscolo descriveremo come ciascuna di queste tecnologie funziona, perché è stata sviluppata, chi la utilizza e come.

Descriveremo inoltre i miglioramenti alla sicurezza da essa apportati, come anche la questione della privacy e altre questioni connesse all'utilizzo di tale tecnologia.

Per questo progetto, e per l'Unione Europea, è importante capire che cosa pensa la gente delle tecnologie per la sicurezza e quanto le ritiene accettabili. Ecco perché la Sua opinione è così importante. Può darsi che Lei sia già nettamente favorevole o contrario ad alcune di queste tecnologie. Durante il focus group dei cittadini SurPRISE Le verranno date molte opportunità di dar voce alla Sua opinione, ma in particolare vorremmo che Lei riflettesse sulle questioni qui sotto indicate.

Che cosa rende una nuova tecnologia per la sicurezza più o meno accettabile per Lei?

Potrebbe essere:

- Conoscere meglio tale tecnologia e il suo funzionamento?
- Saperne di più su come istituzioni diverse utilizzano la tecnologia e i dati che essa produce?
- Sapere che esiste una regolamentazione giuridica efficace e meccanismi di controllo efficaci?
- Avere maggiori informazioni sul tipo di pericoli contro i quali viene impiegata questa tecnologia?

O forse dipende da quanto Lei considera intrusiva questa tecnologia. Ad esempio:

- Causa imbarazzo?
- Viola i diritti fondamentali?
- Rivela informazioni a terzi a Sua insaputa, oppure ha un impatto su altri aspetti della Sua privacy?

Forse dipende da quanto è efficace la tecnologia:

- Rende la vita più comoda?
- La fa sentire più sicuro?
- A Suo parere, individua con precisione le persone sospette?

O forse Lei pensa alle tecnologie per la sicurezza solo quando si rende conto che sono fisicamente vicine a Lei. Ciò potrebbe avvenire quando è in aeroporto, quando è in strada oppure quando usa un cellulare o Internet. Per il resto del tempo non è un problema che La preoccupa. Forse Lei è d'accordo con le tecnologie per la sicurezza adesso, ma è preoccupato per come verranno utilizzate in futuro.

5 TVCC smart

I sistemi TVCC "tradizionali" sono caratterizzati da telecamere montate su installazioni stradali, in luoghi pubblici o negozi. Le telecamere sono collegate a una sala controllo tramite telecomunicazioni. Nella sala controllo numerosi schermi televisivi mostrano a operatori qualificati le immagini catturate dalle telecamere. Tali immagini vengono registrate, memorizzate e, dopo un certo periodo di tempo, cancellate. L'impianto è "chiuso" in quanto le immagini vengono trasmesse esclusivamente alla sala controllo. Se gli operatori vedono qualcosa di sospetto, possono mettersi in contatto con le guardie della vigilanza o con la polizia per telefono o via radio, in modo che possano intervenire.

5.1 Perché è stata messa a punto la TVCC smart

Gli impianti televisivi a circuito chiuso sono stati realizzati originariamente per osservare il lancio di missili durante la seconda guerra mondiale e per gestire a distanza processi industriali rischiosi. Sono stati venduti per la prima volta come tecnologia per la sicurezza negli Stati Uniti negli anni Cinquanta. Sono stati poi adottati dalle forze di polizia a partire dagli anni Sessanta. Nel 2013 gli impianti TVCC sono stati determinanti per individuare i responsabili delle bombe alla maratona di Boston.



La variante "smart" dei sistemi TVCC è stata progettata per risolvere il problema che la TVCC ha dovuto affrontare fin dall'inizio. Si tratta del fatto che ci sono troppe telecamere e troppo pochi occhi per star dietro a tutto ciò che avviene. Contrariamente ad un impianto TVCC "tradizionale", un im-

pianto TVCC smart utilizza videocamere digitali collegate in rete a sistemi che sono in grado di analizzare le immagini digitali. Il software analizza ciò che sta accadendo nell'immagine. Se c'è qualcosa di insolito, suona un allarme acustico e l'attenzione dell'operatore TVCC viene attirata sull'immagine. Viene inoltre registrato l'allarme. Le immagini relative a quell'allarme vengono memorizzate su un computer e possono essere facilmente recuperate e condivise.

Il software della TVCC smart può fare molte cose. Perlopiù viene usato per:

- individuare oggetti in un'immagine, ad esempio un'auto, leggendo la sua targa e confrontandola con i dati presenti in un database;
- individuare il volto di una persona quando tale volto appare contro uno sfondo semplice, sgombro. Per identificare la persona, quell'immagine viene confrontata con le immagini conservate in un database di individui noti;
- identificare un bagaglio abbandonato, ma solo se esso si trova in uno spazio vuoto.

Anche se attualmente la TVCC smart non riesce a fare le seguenti cose in modo affidabile, sono in fase di sviluppo dei software per:

- Individuare le persone in una folla tenendo traccia del loro abbigliamento;
- Individuare un comportamento sospetto o insolito nella scena che viene tenuta sotto controllo, come vagabondare qua e là. I comportamenti nell'immagine vengono confrontati con modelli di comportamento noti archiviati in un database.

Ma non tutti gli impianti di TVCC smart sono uguali. Quanto un impianto sia "smart" dipende dalla bontà del software nell'analizzare l'immagine e da che cosa avviene all'immagine una volta che è stata condivisa. Gli impianti vengono installati per scopi diversi, per cui un impianto di TVCC smart potrebbe non essere in grado di fare tutto ciò di cui si è parlato sopra. Il proprietario dell'impianto potrebbe non avere bisogno che esso faccia tutte quelle cose.

5.2 Come viene usata la TVCC smart

Gli impianti televisivi a circuito chiuso 'intelligenti' sono prodotti e venduti da aziende che producono tecnologie della sicurezza per la difesa. Sono già disponibili numerosi sistemi. Attualmente i principali utenti istituzionali di TVCC smart sono le autorità del settore dei trasporti, come autorità autostradali, aeroportuali, portuali, ferroviarie, enti locali e polizia.

Ad esempio, a Budapest alla fine del 2012 la polizia iniziò ad usare TVCC smart per tenere sotto osservazione le corsie degli autobus. La polizia può legittimamente utilizzare le immagini per punire coloro che viaggiano indebitamente su tali corsie.

L'Unione Europea ha finanziato 16 distinti progetti per sviluppare gli algoritmi e le funzioni degli impianti di TVCC smart. Attualmente sono in fase di sviluppo e di ottimizzazione utilizzi più complessi, come il riconoscimento di comportamenti sospetti o di volti in mezzo alla folla. Il loro impiego non è diffuso e continuano a essere testati nuovi sistemi. Ad esempio, le aziende di trasporto pubblico di Roma, Londra, Parigi, Bruxelles, Milano e Praga hanno partecipato recentemente a sperimentazioni relative a un impianto di videosorveglianza intelligente dei pedoni che utilizza la TVCC smart. Questo sistema avverte gli operatori in presenza di

pacchi sospetti, movimenti anomali da parte dei passeggeri e comportamenti insoliti. Non è operativo perché nel momento in cui scriviamo è ancora in fase di sperimentazione.

Forse l'impiego più diffuso della TVCC smart è il riconoscimento automatico delle targhe auto (di seguito ANPR). Con un'immagine digitale di una targa è possibile confrontarne i dati con i database nazionali dei proprietari di auto, con le banche dati delle assicurazioni e con le banche dati della polizia. È possibile identificare facilmente il proprietario dell'auto e l'indirizzo registrato dell'auto stessa, e la telecamera ANPR è in grado di localizzare uno specifico individuo nel tempo e nello spazio. Il sistema può essere utilizzato per identificare veicoli rubati, veicoli circolanti senza aver pagato imposte o assicurazioni oppure veicoli che procedono a velocità eccessiva.

Una questione è se questi diversi tipi di reati o infrazioni meritino lo stesso tipo di sorveglianza. La TVCC smart dovrebbe essere usata per tutti i tipi di illecito oppure solo per i reati più pericolosi? In Europa esistono pareri discordanti su questo argomento. In Germania, per esempio, nel 2008 la Corte costituzionale ha limitato l'utilizzo delle ANPR da parte della polizia per motivi di privacy. La Corte ha insistito sul fatto che le forze di polizia

Come funziona la TVCC smart

Usando algoritmi intelligenti, un computer collegato a un impianto di videosorveglianza smart impara a riconoscere determinati tipi di comportamento pubblico denominati '*trigger events*' ossia 'eventi scatenanti', come una persona che impugna una pistola, oppure ferma tra la folla in movimento. Un algoritmo è un insieme di calcoli che seleziona i dati contenuti nell'immagine digitale. Un algoritmo intelligente è un algoritmo che impara cosa cercare via via che analizza un numero sempre maggiore di dati.

Gli algoritmi intelligenti degli impianti di TVCC smart sono progettati per replicare il funzionamento dell'occhio e del cervello umano. Il software spezzetta un'immagine in parti piccolissime, denominate pixel. Lei conosce già il termine pixel se possiede una fotocamera digitale o uno smartphone. Se una fotocamera digitale ha 8 megapixel, ciascuna immagine che essa cattura contiene fino a 8 milioni di pixel.

L'algoritmo riesce poi a calcolare il grado di movimento per ciascun pixel nell'immagine. Ciò permette al software di individuare le aree attive in ciascuna scena. Da questo esso impara a riconoscere i modelli di movimento in un'immagine. L'impianto può allora identificare e classificare i fatti secondo i modelli che già conosce. Il software, ad esempio, è in grado di distinguere tra spettatori passivi e tifosi che saltellano durante una partita di calcio.

dovevano conservare i dati digitali raccolti da telecamere ANPR solo in caso di necessità di un loro utilizzo in relazione a un caso concreto. Le ANPR vengono usate anche per far pagare i pedaggi autostradali, ma anche questo ha attirato delle critiche, in quanto per l'applicazione dei pedaggi erano disponibili mezzi diversi, meno orientati alla sorveglianza.

5.3 Miglioramenti relativi alla sicurezza

LA TVCC smart è in grado di migliorare la sicurezza nei modi sotto descritti.

E' più facile individuare i problemi di sicurezza nel momento in cui si generano:

- Il sistema individua tutto ciò che è insolito e allerta l'operatore video con un allarme. Ciò rende più facile per l'operatore interpretare le immagini.
- Gli allarmi rendono più facile per l'operatore decidere in modo più rapido ed efficiente se intervenire o meno per affrontare un problema di sicurezza.
- Gli algoritmi del sistema possono talvolta cogliere dettagli che potrebbero sfuggire agli operatori. Questo perché gli algoritmi sono in grado di trattare volumi molto elevati di dati.

Diminuisce il timore di reati e di intrusione:

- Quando la tecnologia per la sicurezza funziona efficacemente, la gente si rassicura, perché sa che tutto ciò che di solito le avviene intorno verrà individuato rapidamente dal sistema TVCC smart.
- Le telecamere digitali della TVCC smart sono in grado di vedere con un grado di dettaglio molto maggiore rispetto alle telecamere TVCC tradizionali. Ciò significa che per monitorare uno spazio occorrono meno telecamere. La sorveglianza con TVCC smart può essere quindi avvertita come meno intrusiva in quanto sono presenti meno telecamere.
- La privacy può essere accresciuta in quanto aree sensibili delle immagini, come vedute di proprietà private, possono essere "oscurate" in modo che l'operatore non le veda.

5.4 Problematiche

Occorre tener presenti numerosi svantaggi della TVCC smart.

Gli algoritmi della TVCC smart attualmente utilizzati presentano una serie di problemi e punti deboli. Questi ultimi possono produrre un falso allarme che identifica in modo errato un incidente relativo alla sicurezza. Ciò potrebbe significare confondere un innocente con un sospetto. Gli attuali punti deboli sono elencati sotto.

- È possibile tenere sott'occhio in modo affidabile solo certi tipi di oggetti, come la targa di un'auto o un bagaglio abbandonato in uno spazio vuoto.
- Le telecamere sono meno capaci di identificare ciò che avviene nella folla.
- Certi reati, come il borseggio o il taccheggio, sono difficili da individuare.
- Gli algoritmi sono suscettibili di distorsioni, perché sono programmati da esseri umani in modo da individuare ciò che essi considerano come anomalo. Esiste il pericolo che i sistemi possano, deliberatamente o accidentalmente, essere programmati in modo da controllare le minoranze in modo discriminatorio.
- Se, in futuro, un potenziale criminale saprà che in quel momento è in funzione una TVCC smart, potrà evitare di essere rintracciato semplicemente cambiandosi d'abito, in quanto gli algoritmi funzionano riconoscendo gli abiti che i sospetti stanno indossando.
- L'alto livello di falsi allarmi inviati agli operatori umani potrebbe far perdere loro fiducia nel sistema e ignorare ciò che esso sta comunicando.

Le telecamere della TVCC smart sono più potenti e più piccole. Questo comporta le seguenti conseguenze:

- Sono in grado di catturare più informazioni e quindi, potenzialmente, sono più intrusive per la privacy, in quanto è più probabile che catturino e analizzino le attività di persone innocenti.
- Le telecamere sono meno facilmente individuabili, rendendo difficile alle persone sapere che sono sotto la sorveglianza della TVCC smart. Di conseguenza è meno facile per loro sottrarsi o contestare la sorveglianza.

- Può darsi che la libertà di espressione e la dignità della persona vengano lese se il comportamento della gente negli spazi pubblici viene monitorato da questa combinazione di software e operatori umani.

Gli impianti sono ancora azionati da esseri umani.

Ciò significa almeno due cose:

- È un essere umano che deve interpretare l'immagine e confermare che l'allarme sia reale. Anche se il sistema può individuare un comportamento insolito, esso non spiega perché quel comportamento è in corso.
- Occorre che le istituzioni siano regolamentate molto rigidamente su questi tipi di ricerca e che esistano strumenti di tutela contro l'abuso dei dati.

6 Droni

Un drone è l'elemento volante di un sistema aeronautico senza pilota a bordo (UAS). È comandato da un pilota attraverso un sistema di comando a terra oppure vola autonomamente grazie all'utilizzo di un computer di bordo. In inglese i droni vengono chiamati anche aeromobile a pilotaggio remoto (ROA), veicolo a pilotaggio remoto (RPV) oppure velivolo senza pilota (UAV). L'impiego dei droni ha richiamato sempre più l'attenzione del pubblico dopo che gli Stati Uniti hanno iniziato ad usare un numero sempre maggiore di droni nella loro guerra contro il terrorismo in Afghanistan, Pakistan, Yemen e Somalia a seguito degli attacchi terroristici dell'11 settembre. Molti stati europei stanno riarmando le loro forze militari con droni.

I droni vengono usati non solo dai militari in un contesto bellico, ma anche dalle forze dell'ordine a fini di ricognizione e sorveglianza, per garantire la sicurezza dei cittadini. Questi droni 'civili' vengono sempre più usati come telecamere volanti che tengono sotto controllo gli spazi pubblici per prevenire o individuare un'ampia gamma di minacce per la sicurezza. I droni civili vengono impiegati anche per scopi non connessi alla sicurezza, come cartografia e fotografia immobiliare o come giocattoli. Un altro aspetto importante è che essi permettono di sorvegliare aree che sono troppo pericolose per l'accesso di esseri umani, ad esempio dopo valanghe, terremoti o incidenti nucleari. I droni, ad esempio, sono stati usati dopo l'incidente di Fukushima sia per monitorare lo stato dell'impianto che per controllare il livello di radiazioni.



Poiché il progetto SurPRISE esplora le capacità delle tecnologie per la sicurezza orientate alla sorveglianza, esistenti ed emergenti, di promuovere la sicurezza, in questa sede parleremo soprattutto dei droni civili utilizzati a fini di sicurezza.

6.1 Perché sono stati realizzati i droni

Inizialmente i droni furono progettati per scopi di ricognizione militare e di attacco mirato con armamenti. La tecnologia del pilotaggio remoto di un aeromobile senza pilota a bordo fu impiegata per la prima volta durante la prima guerra mondiale. Il primo veicolo fu ideato dal prof. A. M. Low in Gran Bretagna nel 1916. Esso fu progettato sia come difesa contro gli Zeppelin comandati da terra sia come bomba volante comandata da un aereo con pilota a bordo che accompagna il drone.

Anche se oggi i droni sono associati perlopiù ad azioni militari, essi vengono sempre più utilizzati da organismi governativi civili, da aziende e da privati.

All'interno della UE l'uso di droni 'leggeri', dal peso inferiore a 150 kg, e l'utilizzo di tutti tipi di droni per scopi di sicurezza o militari sono regolamentati dagli stati membri. La regolamentazione dell'uso di droni di grandi dimensioni per scopi commerciali è attualmente all'esame della Commissione Europea, che punta ad iniziare l'integrazione dei droni nello spazio aereo civile UE nel 2016. Nel 2028 i droni dovrebbero essere pienamente integrati nello spazio aereo civile della UE.

Le ricerche attuali puntano a rendere i droni futuri ancora meno dipendenti dalla supervisione umana, valicando così il confine con le scienze robotiche. I droni vengono equipaggiati di sensori che permettono loro di volare autonomamente nello spazio urbano. Si stanno sviluppando anche nuove modalità di produzione di massa di micro-droni. Le capacità tecnologiche nel settore dei droni crescono rapidamente, perché i costi di costruzione e di utilizzo diminuiscono continuamente.

I droni possono essere dotati di tutta una serie di attrezzature aggiuntive, che permettono sia la sor-

veglanza che l'intervento. Le aggiunte possibili dipendono dalle dimensioni e dalla capacità di carico utile del singolo veicolo.

6.2 Come vengono usati i droni

I droni possono integrare efficacemente l'infrastruttura esistente (aerei con pilota a bordo o satelliti) ed essere utilizzati da organismi pubblici nei settori della gestione delle crisi, del mantenimento dell'ordine pubblico, del controllo delle frontiere, del monitoraggio del traffico o delle operazioni antincendio.

Nell'ambito della sicurezza, le forze dell'ordine nell'UE usano i droni soprattutto per monitorare gli assembramenti di persone in grandi eventi pubblici, come dimostrazioni ed eventi sportivi, allo scopo di individuare fatti insoliti o movimenti improvvisi della folla. Possono essere usati anche per indagini sulla scena di un delitto. Il loro utilizzo nel controllo delle frontiere è un'altra possibilità che verrà sfruttata nella UE nel prossimo futuro. I droni sono stati usati anche per scoprire coltivazioni di droga e sostenere la polizia nelle sue inda-

gini.

I droni di sorveglianza utilizzati per monitorare gli spazi pubblici hanno un enorme vantaggio comparativo. Sono in grado di monitorare uno spazio molto più grande, sono mobili e il loro utilizzo ad un'altezza che va dai 50 ai 200 metri permette una prospettiva diversa rispetto alla maggiore staticità delle videocamere di sorveglianza (TVCC) pubbliche.

I droni possono essere usati per un'ampia gamma di applicazioni commerciali. Posso essere impiegati a supporto dell'agricoltura e della pesca di precisione, per il monitoraggio delle linee elettriche e del gas, per l'ispezione di infrastrutture, per servizi di telecomunicazione e radiotelevisivi, per comunicazioni wireless e per il potenziamento dei sistemi satellitari, per il monitoraggio delle risorse naturali, per l'industria dell'intrattenimento mediatico, per la mappatura digitale, per la gestione territoriale e faunistica o per la gestione e il controllo della qualità dell'aria.

Malgrado tali straordinarie prospettive, varie que-

Come funzionano i droni

I droni sono prodotti in un'ampia gamma di formati e sono in grado di trasportare una quantità virtualmente illimitata di 'carichi utili', cioè di oggetti attaccati al drone, come telecamere, sensori o missili. Di solito i droni vengono comandati a distanza da uno o più operatori che controllano e monitorano da terra le attività del veicolo e i suoi carichi utili. È possibile comandare un drone con uno smartphone o un tablet. In qualche caso può essere possibile pre-programmare un drone per una rotta di volo specifica all'interno del suo range di volo. Tuttavia, rispetto al pilotaggio remoto, la programmazione autonoma di tali droni è ancora agli inizi ed è al centro della ricerca attuale. La comunicazione tra un drone e il suo operatore può avvenire in varie forme, anche se, per le lunghe distanze, può essere necessario il collegamento ad un satellite per supportare la trasmissione di dati dal veicolo e inviare comandi di risposta.

Un sistema UAV è costituito tipicamente da questi elementi:

- aeromobile senza pilota a bordo (UAV);
- unità di comando a terra, eventualmente mobile;
- collegamento dati, eventualmente con supporto satellitare;
- equipaggiamento aggiuntivo.

Dimensioni e attrezzatura dei droni variano molto a seconda degli scopi per cui vengono utilizzati. I droni, ad esempio, possono essere equipaggiati con telecamere a circuito chiuso, sensori, telescopi, radar, Wi-Fi e altre tecnologie di intercettazione delle comunicazioni, con rilevatori di sostanze chimiche o radiazioni e con armi. Poiché gran parte della ricerca è incentrata sullo sviluppo di micro-droni o nano-droni in grado di imitare il movimento di insetti e uccelli, si può prevedere che in futuro la capacità di sorveglianza dei droni sarà quasi illimitata, anche se gli scenari di utilizzo consentiti sono ancora piuttosto limitati a causa delle restrizioni legali.

stioni tecniche relative ai droni rimangono ancora irrisolte. Tali questioni riguardano, ad esempio, i limiti relativi ad altitudine, velocità e durata del volo, come pure problematiche emergenti riguardanti il rifornimento di carburante in volo. I droni sono inoltre molto vulnerabili alle condizioni atmosferiche sfavorevoli, come nuvole pesanti, vento e pioggia. Inoltre i droni che generano dati grazie ad un equipaggiamento avanzato, come telecamere a circuito chiuso o sensori, causano problemi di carico e di segnale dovuti alla mancanza di larghezza di banda. Le riprese video possono risultare sfocate a causa del movimento del drone.

6.3 Miglioramenti della sicurezza

1. I droni rendono più facile individuare problemi per la sicurezza.
 - I droni sono in grado di monitorare aree grandi e/o inaccessibili. In uno scenario di ricerca e salvataggio, ad esempio, i droni possono essere usati per sorvegliare grandi aree inaccessibili come le foreste fitte. I droni riescono anche a monitorare grandi aree confinarie per individuare ingressi non autorizzati e combattere il traffico di esseri umani.
 - I droni sono mobili: riescono non solo a individuare e registrare oggetti e individui sospetti, ma a tenere traccia di essi quando si muovono in spazi pubblici. Contrariamente alle squadre umane che seguono individui od oggetti, i droni sono instancabili e meno visibili, per cui riescono a dare la caccia ad oggetti e individui per un lungo periodo di tempo.
 - I droni sono meno visibili delle telecamere a circuito chiuso. Di conseguenza è più difficile che vengano scoperti dai potenziali malviventi.
2. La paura di reati e di intrusione nella vita privata si riduce.
 - Quando la gente sa che una specifica area è tenuta sotto controllo da un drone, potrebbe sentirsi rassicurata, perché sa che qualunque fatto insolito avvenga lì intorno verrà individuato rapidamente dal drone.

6.4 Problematiche

1. I droni sono meno visibili rispetto alle telecamere a circuito chiuso o ai sensori, per cui riescono a registrare e archiviare informazioni in modo indiscriminato. Ciò li rende uno strumento potenzialmente più invasivo per la privacy.
 - Le capacità di droni superano quelle delle TVCC smart, perché i droni riescono a raccogliere informazioni da luoghi privati che i singoli hanno cercato di impedire venissero visti, ad esempio costruendo muri, recinzioni o altro. I droni sono quindi in grado di ottenere immagini di proprietà private che non sono visibili per le TVCC statiche.
 - Come la maggior parte delle tecnologie per la sorveglianza, anche i droni hanno la capacità di registrare e archiviare informazioni in modo indiscriminato. E' quindi più probabile per loro catturare e analizzare le attività pubbliche e private di persone innocenti. Ciò può produrre un effetto intimidatorio e dissuasivo.
 - Rispetto alle TVCC, i droni sono ancora meno facili da individuare, e ciò rende più difficile alle persone sapere che in quel momento vengono monitorate. Il carattere intrinsecamente mobile dei droni rende difficile scoprire chi esattamente li sta azionando. Di conseguenza è meno facile per i cittadini opporsi alla sorveglianza od evitarla.
 - Questa difficoltà può far scattare una sensazione permanente di incertezza negli individui oggetto di osservazione, causando cambiamenti più o meno lievi nel loro comportamento per evitare un'attenzione indesiderata e negativa. L'effetto intimidatorio e dissuasivo sopra menzionato diverrà ancora più forte una volta che droni saranno stati sempre più equipaggiati con caratteristiche di "TVCC smart", come funzionalità di riconoscimento basato sullo schema comportamento/anomalia, che può colpire pesantemente l'esercizio di diritti fondamentali come la libertà di espressione e la libertà di associazione in spazi pubblici.

- L'uso di droni in combinazione con TVCC statiche a terra e dispositivi di localizzazione consente una sorveglianza molto più completa dei cittadini, rendendo possibile realizzare un profilo dettagliato dei loro movimenti, del loro comportamento personale e sociale.
2. I droni equipaggiati con dispositivi di registrazione dati come TVCC o sensori possono essere vulnerabili ad hacker esterni a causa di mancata crittazione dei dati e di interruzioni nelle comunicazioni verso la base o verso il pilota.
 3. Esistono inoltre questioni di sicurezza pubblica connesse all'utilizzo dei droni in zone abitate.
 - I droni hanno un tasso di incidenti molto superiore a quelli dei velivoli con pilota a bordo, perché sono più suscettibili alle condizioni atmosferiche (vento, pioggia). Ciò aumenta il rischio per le persone a terra.

7 Cybersorveglianza mediante Deep Packet Inspection (DPI)

I fornitori di servizi Internet, gli operatori delle reti di telecomunicazione e le aziende di telecomunicazione sono sempre stati in grado di monitorare le proprie reti. Sapere chi sta comunicando con chi, quali siti web vengono visitati e quali servizi vengono utilizzati sono elementi indispensabili per la fatturazione al cliente, la gestione delle reti e le attività di marketing di queste società. Adesso,

però, una tecnica chiamata DPI permette alle aziende, alle agenzie di spionaggio e ai governi di arrivare al contenuto delle comunicazioni inviate via Internet. Volendo fare un'analogia, il DPI equivale a un servizio postale che apre tutte le lettere, le legge e talvolta le modifica, le cancella o non le consegna.

Come funziona il DPI

L'invio o la ricezione di informazioni su Internet costituisce un processo molto complesso, che passa attraverso numerosi computer.

I computer collegati attraverso il web spezzettano le informazioni che vengono inviate o ricevute in insiemi più piccoli chiamati "pacchetti". Ciò permette alle informazioni di viaggiare facilmente attraverso Internet. Quando i pacchetti arrivano a destinazione, vengono rimessi insieme, come una sorta di puzzle, ricostituendo il messaggio. Ciascun pacchetto ha un'etichetta chiamata "header", che descrive che cos'è il pacchetto, da chi proviene e dove sta andando, proprio come una lettera inviata attraverso la rete postale. All'interno del pacchetto c'è il contenuto del messaggio, che viene chiamato "payload" [carico utile].

Ciascun pacchetto è formato da più strati, ciascuno dei quali contiene informazioni diverse sul messaggio. Gli strati sono collocati uno dentro l'altro, un po' come in una matrioska. Perché il messaggio possa essere recapitato è necessario che il fornitore di servizi Internet ispezioni alcuni dei pacchetti che lo compongono. La maggior parte delle volte occorre guardare solo gli header (corrispondenti all'esterno della busta) e non il payload (ciò che è contenuto nella busta) per essere certi che il messaggio venga recapitato. Questa procedura è denominata "shallow packet inspection", cioè "ispezione pacchetti superficiale". L'ispezione pacchetti approfondita (il DPI), invece, comprende l'ispezione di tutti pacchetti di un messaggio e l'esame non solo degli header ma anche dei payload.

I pacchetti vengono ispezionati utilizzando algoritmi in grado di scansionare i messaggi per individuare particolari tipi di dati. Nella descrizione della TVCC smart abbiamo descritto gli algoritmi come insiemi di calcoli che selezionano e analizzano i dati. Vengono usati anche nel DPI, ma in modo diverso.

Nel DPI un algoritmo viene programmato per cercare parole chiave specifiche, in modo analogo a quando si cercano informazioni in un motore di ricerca. Il tipo di dati cercati dipende da chi sta facendo la ricerca e dal perché la sta facendo. Le parole chiave utilizzate possono riferirsi ad attività criminali o sospette, a nuovi virus circolanti in rete, o addirittura all'acquisto o meno di un determinato prodotto.



Il DPI è in grado di monitorare ogni aspetto della comunicazione digitale, dalle informazioni che Lei legge on-line, dai siti web da Lei visitati, dai video che Lei guarda e dalle parole che ricerca fino alle persone con cui Lei comunica via e-mail, *instant messaging* o *social media*. Le applicazioni DPI possono aprire e analizzare i messaggi mentre questi sono in viaggio, identificando quelli che possono comportare particolari rischi. Non è necessario che Lei sia una persona sospetta per cadere sotto la scansione di sistemi DPI – il DPI intercetta e legge ogni messaggio che viaggia sulla rete di un fornitore di servizi Internet.



7.1 Perché è stato messo a punto il DPI

In origine il DPI è stato sviluppato per scoprire virus e malware che danneggiano le reti informatiche. Oggi, usando il DPI per analizzare il contenuto dei messaggi mentre sono in viaggio, è possibile non solo fermare i virus, ma individuare anche l'attività dolosa, pericolosa o criminale che avviene tramite Internet.

Tutte le apparecchiature nelle quali è alloggiata la tecnologia che esegue il DPI sono di proprietà delle società di Internet. Tali società sono in grado di controllare il funzionamento di Internet a livello locale, regionale, nazionale o internazionale. Queste società intendono usare la tecnologia per i pro-

pri fini, ma possono anche ricavare denaro vendendo la loro innovazione ad altri. Anche altre società, come le aziende che lavorano per la Difesa, hanno sviluppato una tecnologia DPI e desiderano fare lo stesso. Attualmente esiste un mercato per la tecnologia DPI.

7.2 Come viene usato il DPI

In Europa il DPI può essere usato legalmente solo in misura molto limitata. Secondo le leggi esistenti, può essere usato per "filtrare" il traffico Internet, vagliandolo per individuare eventuali virus e malware. Può inoltre aiutare le *internet companies* a gestire il flusso di traffico sulle proprie reti. Ma la tecnologia DPI è in grado anche di analizzare tutto il contenuto delle comunicazioni on-line. Quando viene usata in questo modo, è in grado di scoprire reati molto specifici, come la distribuzione di pedopornografia. Ma ciò è legalmente controverso, in quanto non esiste alcuna legge specifica che disciplini questo uso "in dettaglio" del DPI. Questo avviene perché le leggi europee sulle tecnologie per la comunicazione sono state redatte quando il DPI ancora non esisteva. La Corte di giustizia europea e il Garante europeo della protezione dei dati hanno interpretato queste leggi dicendo che esse si riferiscono solo al "filtraggio" limitato di comunicazioni on-line. Occorre mettere a punto nuove leggi che permettano di disciplinare adeguatamente l'uso più dettagliato del DPI.

Il DPI non può quindi essere legalmente utilizzato per monitorare le comunicazioni in generale, per scoprire violazioni di diritti d'autore, per bloccare contenuti politicamente sensibili o per individuare target pubblicitari, anche se è una tecnologia in grado di fare tutte queste cose. Le leggi europee tutelano la riservatezza delle comunicazioni. Il DPI violerebbe anche la Convenzione europea dei diritti dell'uomo, in quanto prevede una sorveglianza di massa priva di garanzie e senza obiettivi specifici: può essere letto ogni bit delle informazioni che vengono inviate e ricevute tra computer.

Il quadro è molto diverso negli USA, dove non è regolamentata e molte aziende la usano per individuare obiettivi pubblicitari. Se Lei ha un indirizzo e-mail Gmail o Yahoo, il messaggio viaggerà quasi sicuramente attraverso gli USA e sarà sottoposto al

DPI. A quanto pare, il DPI è stato usato in connessione con i programmi di sorveglianza di massa della NSA (Agenzia per la sicurezza nazionale) statunitense e del GCHQ (Quartier Generale Governativo per le Comunicazioni) britannico, svelati nell'estate 2013.

Esiste un vuoto legislativo sulle modalità con cui rilevare, controllare e limitare l'uso del DPI: la regolamentazione stenta a stare al passo con le innovazioni tecnologiche. È comunque difficile capire la misura in cui il DPI è usato: ogni messaggio da Lei inviato o ricevuto può viaggiare in tutto il mondo prima che arrivi a destinazione. Potrebbe essere stato analizzato da sistemi DPI utilizzati da un fornitore di servizi Internet, da un governo oppure dai servizi di sicurezza di un certo numero di paesi; è quasi impossibile dare una risposta definitiva in proposito. L'assenza di regolamentazione genera una situazione di caos; tanto le compagnie quanto i governi potrebbero approfittare di questo vuoto legislativo.

Ciò che possiamo dire è che in tutto il mondo molte istituzioni diverse utilizzano il DPI. I fornitori di servizi Internet, società di marketing, la polizia e le agenzie di sicurezza dei governi nazionali l'hanno utilizzata in momenti diversi. L'anno scorso sono stati rivelati alcuni impieghi del DPI al di fuori delle ampie attività di sorveglianza delle agenzie di sicurezza USA rivelate dall'informatico Edward Snowden: alcuni sono commerciali, altri si riferiscono alla sicurezza pubblica e nazionale.

7.2.1 Usi commerciali

- *Sicurezza e gestione della rete.* I messaggi vengono ispezionati per accertarsi che non contengano virus, e spesso viene filtrato il file sharing P2P, cioè la condivisione di grossi files da persona a persona.
- *Pubblicità comportamentale.* Dai messaggi vengono raccolti dati relativi ai prodotti preferiti da una persona. Ciò non è consentito in Europa, ma è apprezzato da alcuni consumatori negli USA, dove questa prassi è permessa, perché consente loro di accedere a prodotti e servizi appropriati alle loro necessità.
- *Gestione dei diritti digitali.* I messaggi vengono ispezionati per individuare la condivisione illegale di file e la violazione di diritti d'autore.

7.2.2 Impieghi per la sicurezza pubblica e nazionale

Sorveglianza governativa sulle attività criminali. Il DPI viene proposto come strumento investigativo in relazione a reati molto specifici, anche se ciò è legalmente controverso. Si tratta di reati:

- commessi contro computer o utilizzando computer (ad esempio la distribuzione di pedopornografia);
- consistenti nella condivisione di informazioni razziste o in minacce di stampo razzista;
- relativi all'incitamento al terrorismo o all'organizzazione di atti terroristici;
- relativi alla condivisione di informazioni che inneggiano al genocidio o ai crimini contro l'umanità.

Censura. Si è sostenuto che il DPI sia stato usato contro gli oppositori politici nei regimi repressivi di tutto il mondo. La NARUS, un'azienda statunitense del settore della Difesa, consociata della Boeing, ha venduto sistemi DPI alla Libia, che l'ha usato per schiacciare il dissenso durante la primavera araba. Al contrario, all'alba della primavera araba la Gran Bretagna ha limitato la vendita di tecnologia DPI all'Egitto, al Bahrein e alla Libia revocando le licenze di esportazione. Anche se il fornitore della tecnologia non è noto, l'Iran sta usando il DPI non solo per spiare e censurare le informazioni alle quali i cittadini possono accedere on-line, ma anche per alterare il contenuto online e creare così disinformazione. Anche la Cina utilizza il DPI in modo analogo. Non si sa se anche all'interno dell'Europa Internet venga censurato.

7.3 Miglioramenti della sicurezza

Il DPI è in grado di migliorare la sicurezza delle informazioni e la lotta contro il crimine individuando e bloccando messaggi dannosi o criminali, come quelli descritti nel paragrafo precedente.

Anche se il DPI non è in grado di prevenire i gravi reati ai quali si riferiscono questi messaggi, esso permette di scoprirli e può fornire prove concrete in un'indagine. Esso, invece, è effettivamente in grado di prevenire la diffusione di virus e di altre forme di criminalità informatica.

7.4 Problematiche

Il DPI solleva una serie di gravi questioni.

1. Il DPI vede tutto.
 - Può analizzare tutti i messaggi e tutti i dati sensibili in essi contenuti mentre viaggiano, il che significa che con il DPI le comunicazioni elettroniche non sono più private.
 - Sapere che le comunicazioni non sono più private potrebbe avere un serio effetto intimidatorio e dissuasivo, cioè le persone temono di comunicare apertamente e di esprimersi liberamente.
 - L'uso del DPI deve essere disciplinato molto rigorosamente, perché esso ha un enorme potere.
2. Le capacità tecnologiche cambiano più rapidamente delle leggi.
 - Non esistono norme giuridiche chiare in merito a ciò per cui il DPI può o non può essere usato.
 - In pratica, l'uso del DPI dipende dall'etica di chi lo sta usando. Può essere utilizzato per qualsiasi cosa, dall'individuazione di virus del computer all'oppressione politica.
 - Nei paesi nei quali esiste uno stretto rapporto tra governo nazionale e fornitori nazionali delle comunicazioni, le informazioni potrebbero essere condivise in modo da dare allo Stato l'accesso a tutte le comunicazioni elettroniche fatte dai cittadini.
3. È difficile localizzare esattamente chi sta usando il DPI e dove.
 - Le norme giuridiche dovrebbero essere uguali ovunque. Da qualche tempo le autorità garanti della privacy in tutto il mondo stanno chiedendo uno standard minimo internazionale di privacy.
4. L'efficacia del DPI è discutibile.
 - Un "regolamentatore" del DPI dovrebbe essere un ente veramente internazionale con potere sufficiente a punire i trasgressori.
 - I computer identificano solo i messaggi potenzialmente problematici, quindi esiste la questione degli errori di interpretazione e delle persone innocenti che diventano dei sospetti.
 - Alcuni esperti hanno criticato l'incapacità del DPI di individuare materiali illegali.

8 Geolocalizzazione degli smartphone

Gli smartphone hanno quasi eclissato il coltellino svizzero come strumento e giocattolo perfetto, tutto in uno. Nel mondo ci sono grosso modo 5 miliardi di cellulari, per una media di quasi 1,3 cellulari per persona. È un numero enorme, se si pensa che questo tipo di telefono è divenuto disponibile solo alla fine degli anni Novanta.

8.1 Perché è stata sviluppata la geolocalizzazione degli smartphone

Gli smartphone costituiscono uno sviluppo relativamente recente. La loro enorme popolarità è dovuta al fatto che sono in grado di fare molte cose diverse, oltre che essere un normale telefono cellulare. In effetti gli smartphone somigliano più a piccoli computer tascabili ai quali di tanto in tanto viene chiesto di fare una telefonata. Come qualsiasi computer fisso o portatile, ciascun tipo di smartphone ha il proprio sistema operativo, che permette di inviare e-mail, messaggi e navigare in Internet. Sugli smartphone possono girare applicazioni software in grado di fornire servizi come giochi, mappe e notizie on-line. Hanno anche videocamere digitali, *media player* portatili e hanno schermi più grandi, a colori, azionabili con il tocco di un dito.

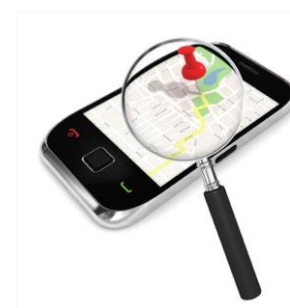
Le origini dei telefoni cellulari risalgono alla seconda guerra mondiale. Fondamentalmente un cellulare è una radio senza fili in grado di inviare e ricevere messaggi. Le prime radio senza fili, i walkie talkie, furono introdotte per aiutare i soldati a rimanere in contatto con la linea del fronte. Negli anni Settanta e Ottanta le innovazioni nei microprocessori videro emergere i primi telefoni portatili. Originariamente il telefono cellulare aveva le dimensioni e il peso di un mattone e la batteria aveva un'autonomia di soli 20 minuti. Come sono cambiati i tempi! A partire dagli anni Ottanta una rete crescente di antenne per telefonia mobile ha migliorato i segnali sia localmente sia sulle distanze più lunghe.

Le antenne sono molto importanti nella localizzazione dei cellulari. Un'antenna copre una determinata area geografica. Per potersi collegare alla rete, fare telefonate o inviare messaggi, tutti i cellulari

devono registrarsi presso l'antenna telefonica più vicina. L'antenna alla quale si collegano registra sempre la loro posizione. Se la persona che usa il cellulare si sposta nell'ambito di un'antenna diversa, il telefono si registra presso quest'ultima. Il movimento di una persona che ha con sé un cellulare viene quindi tracciato dal fornitore dei servizi di telecomunicazione. Nell'Unione Europea le normative attuali esigono che gli operatori conservino questi dati per un periodo che va da un minimo di 6 a un massimo di 24 mesi. La relativa direttiva UE è stata rigettata dalla Corte di Giustizia europea nell'aprile 2014, ma finora le normative nazionali non sono cambiate.

Lo smartphone può essere localizzato anche in altri modi. La persona che lo utilizza può impostarlo in modo che esso stabilisca la propria posizione usando il GPS (satelliti di posizionamento globale) e collegandosi alle reti wireless.

Ciò ha portato a un'enorme crescita della fornitura di "servizi di geolocalizzazione" per gli smartphone. Di solito sono disponibili come applicazioni ("app") che possono essere installate sul telefono. Una app è un software in grado di svolgere una specifica funzione o servizio. Le app di geolocalizzazione



permettono all'utente di trovare informazioni su ristoranti o negozi situati nelle vicinanze, oppure scoprire quale dei suoi amici si trova più vicino a lui. Ora sono disponibili anche giochi basati

sulla geolocalizzazione. Probabilmente questo tipo di servizi sarà sempre più utilizzato nei prossimi anni.

I servizi di geolocalizzazione offrono molto a chi usa lo smartphone. Tuttavia, per alcuni difensori della privacy, il livello di informazioni che può essere rivelato dalla geolocalizzazione dello smartphone suscita preoccupazione. Quando, ad esempio, il politico tedesco Malte Spitz, dei Verdi, entrò in possesso delle registrazioni dei dati di

geolocalizzazione del suo cellulare relativi ai sei mesi precedenti, vide che avevano l'aspetto di un flusso continuo di numeri e lettere. Ma quando Malte fece leggere i dati a un esperto di statistica, emerse un quadro dettagliato della sua vita. In collaborazione con il quotidiano *Die Zeit*, Malte realizzò un'animazione che mostrava in dettaglio esattamente dove era stato in quei sei mesi. Malte iniziò a preoccuparsi del livello di dettaglio che poteva essere rivelato a proposito della sua vita, in particolare se i dati di geolocalizzazione fossero stati abbinati a informazioni provenienti da *social*

network come Twitter o Facebook.

In un caso discusso recentemente davanti alla Corte suprema statunitense, il giudice ha osservato che i dati GPS potevano rivelare viaggi "indiscutibilmente privati", aventi come destinazione "lo psichiatra, il chirurgo plastico, la clinica per abortire, il centro per la cura dell'AIDS, il locale di spogliarelli, l'avvocato penalista, il motel a ore, la riunione sindacale, la moschea, la sinagoga o la chiesa, il locale per gay e così via".

Come funziona la geolocalizzazione degli smartphone

Possono essere localizzati sia i cellulari normali sia i cellulari "smart". Esistono tre modi per tracciare un cellulare: attraverso antenne, GPS o reti wireless. La prima modalità vale per tutti i cellulari, mentre la seconda e la terza si applicano solo agli smartphone.

Antenne per telefonia mobile. Tutti i cellulari si registrano presso l'antenna per telefonia mobile più vicina, in modo che telefonate, messaggi ed e-mail possano essere inviati e ricevuti attraverso la rete per telefonia mobile. Ciascun cellulare contiene un numero di riferimento unico ed esclusivo, che collega il telefono a un account presso l'azienda telefonica e quindi all'utente. Queste informazioni sono necessarie anche per emettere le fatture telefoniche. Se servizi di sicurezza o forze dell'ordine cercano di tracciare i movimenti di una specifica persona in un determinato momento, possono richiedere alle aziende telefoniche i dati delle antenne per telefonia mobile. Le registrazioni dell'antenna indicano se il cellulare di quella persona era nell'ambito di ricezione di un'antenna particolare. Facendo questo per tutte le antenne - come richiesto nell'Unione Europea - è possibile individuare la posizione del telefono, scoprendo così i movimenti del suo proprietario.

GPS. Gli smartphone contengono un software di mappatura e applicazioni che funzionano sulla base dei dati di posizionamento globale. Quando viene attivata la funzione GPS di uno smartphone, quest'ultimo elabora la sua posizione sul pianeta calcolando quanto è lontano dai più vicini satelliti GPS che viaggiano nello spazio. Quando il GPS viene spento, il telefono non è in grado di autolocalizzarsi con il GPS. Tuttavia questa caratteristica può essere attivata a distanza all'insaputa dell'utente, ad esempio se sul cellulare è installata una app che permette di localizzarlo se viene perduto o rubato. I fornitori di app raccolgono questi dati di localizzazione e alcuni li vendono a fini commerciali.

Se i servizi di sicurezza e le forze dell'ordine stanno cercando di rintracciare una determinata persona, possono chiedere i dati GPS alle aziende telefoniche.

Wireless. Gli smartphone possono collegarsi alle reti wireless operanti in una determinata area. Il collegamento a una rete wireless localizza il cellulare all'interno dei confini di una rete wireless. Anche in questo caso, disattivare questo collegamento significa che il cellulare non può essere rintracciato utilizzando questa modalità. Tipicamente un punto di accesso Wi-Fi ha una portata di 20 metri all'interno degli edifici, ma una portata maggiore all'aperto.

Possono essere tracciati nello stesso modo anche altri dispositivi mobili "smart", come iPad, tablet e notebook.

8.2 Come viene usata la geolocalizzazione degli smartphone

I dati di geolocalizzazione degli smartphone vengono utilizzati per scopi sia commerciali sia di sicurezza.

8.2.1 Usi commerciali

- *Gestione delle fatture telefoniche.* Le aziende di telefonia mobile hanno bisogno dei dati di localizzazione e del numero di identificazione del cellulare per poter emettere la fattura telefonica.
- *Marketing mirato.* Le società di software che producono app come Twitter, Angry Birds o FourSquare raccolgono dati di localizzazione e altri dati di contatto dai cellulari e li vendono ai pubblicitari. Questi ultimi poi usano i dati per ideare la pubblicità relativa ai prodotti venduti negli spazi che essi sanno essere utilizzati da differenti tipi di consumatori. Il gioco Angry Birds, ad esempio, è stato scaricato un miliardo di volte in tutto il mondo. Gli utenti sono rimasti sorpresi nello scoprire che la società finlandese che lo ha sviluppato, la Rovio Entertainment Ltd, raccoglieva e vendeva di routine i dati di geolocalizzazione dei giocatori. Il 50% di tutte le app raccoglie dati di localizzazione anche quando la app non ha bisogno di questi dati per funzionare.
- *Pianificazione urbanistica.* I dati di geolocalizzazione possono essere usati per mappare l'uso degli spazi urbani. Poiché esistono molte più antenne per telefonia mobile negli spazi urbani che in quelli rurali, i telefoni possono essere tracciati molto più da vicino. Questa foto, dall'aspetto quasi spionistico, è una mappa dell'uso dei cellulari a Graz, in Austria. Ricercatori del Massachusetts Institute of Technology hanno tracciato anonimamente i cellulari per costruire un quadro di come la gente si sposta nella città di Graz; il loro scopo è di informare gli urbanisti e i progettisti del trasporto pubblico sul modo in cui viene usata la città.



8.2.2 Impieghi per la sicurezza pubblica e nazionale

- *Ritrovare persone scomparse e ferite.* Negli Usa e in Canada il servizio E-911 obbliga per legge i cittadini a usare il GPS su tutti i telefoni cellulari, in modo che essi (e i loro utenti) possano essere localizzati in caso di emergenza. In Europa vengono fatte ogni anno circa 180 milioni di telefonate di emergenza. Di queste, il 60-70% parte da cellulari. Il telefono rivela i suoi dati GPS al numero di emergenza 112, valido in tutta Europa. A differenza degli americani e dei canadesi, gli europei non sono obbligati ad avere il GPS sempre acceso sul loro telefono.
- *Tracciare (cioè seguire continuamente) i movimenti di persone sospette.* Le forze di sicurezza e dell'ordine possono accedere ai dati GPS presentando apposita richiesta alle aziende di telefonia mobile. Attualmente in Europa ciascuna di queste richieste è regolamentata per legge. Al ricevimento di tale richiesta, le aziende devono consegnare alle forze dell'ordine tutti i dati relativi a una persona sospetta. I servizi di sicurezza hanno anche altri metodi per rintracciare le telefonate, che possono essere applicate a individui mirati.
- *Tracciare i familiari.* Anche i singoli possono trarre beneficio dei servizi GPS. Molti genitori conoscono bene i prodotti di geolocalizzazione per utenti individuali, che permettono loro, ad esempio, di vedere in qualsiasi momento dove sono i loro figli.

Controversia sulla geolocalizzazione degli smartphone

Dopo le proteste del movimento 'Occupy' a New York, Twitter è stata costretta a fornire al governo USA dati di localizzazione per poter identificare i partecipanti alla protesta. Recentemente Twitter ha lanciato un nuovo servizio che si chiama 'Please Don't Stalk Me' e permette agli utenti di falsare i dati di localizzazione connessi ai loro tweet. Tale app consente agli utenti di segnalarsi in qualunque luogo del pianeta tramite Google Maps e di inserire quei dati falsi nei loro tweet. Fanno lo stesso anche altre app, come 'My Fake Location', 'Fake GPS Location' e 'GPS Cheat'.

8.3 Miglioramenti della sicurezza

La geolocalizzazione degli smartphone migliora la sicurezza in vari modi:

- Permette di trovare e aiutare persone in situazioni di pericolo;
- Permette alle famiglie di tenere sotto controllo adulti vulnerabili o bambini;
- La polizia e altre forze dell'ordine possono usare i dati GPS per collocare individui sulla scena di un crimine o per incriminarli come sospetti. Possono inoltre rintracciare e seguire i sospetti nel corso delle indagini.
- Poiché i dati GPS sono stati usati per identificare i partecipanti alle proteste, il loro uso ha un potenziale effetto intimidatorio e dissuasivo, in quanto gli individui possono diventare cauti e limitare le proteste e l'esercizio dei loro diritti democratici.

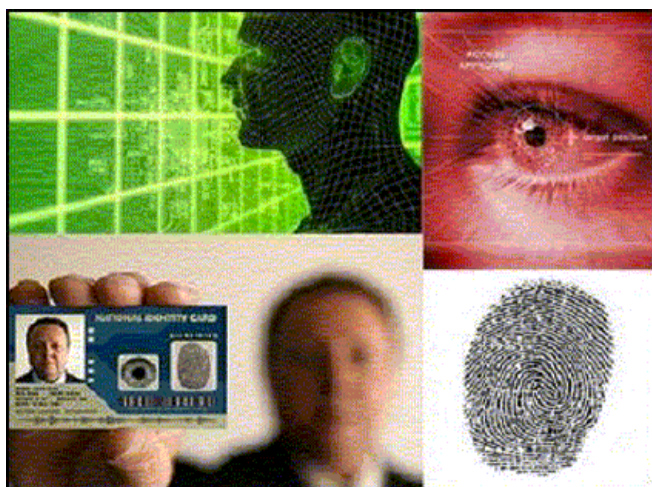
8.4 Problematiche

La geolocalizzazione degli smartphone solleva le seguenti questioni connesse alla privacy, alla regolamentazione e ai diritti umani.

- Gli utenti non hanno il completo controllo delle informazioni rivelate dagli smartphone. Tale controllo è particolarmente difficile per gli utenti più vulnerabili, come i collaboratori di giustizia, che possono non voler condividere i dati GPS ma vorrebbero ancora godere dei vantaggi del cellulare. Alcuni telefoni, come gli iPhone della Apple, archiviano automaticamente i dati di geolocalizzazione e questa funzione non può essere spenta.
- Molte app raccolgono dati di geolocalizzazione anche se la app non ne ha bisogno per funzionare. In assenza di una forte pressione popolare, è improbabile che le aziende telefoniche offrano ai consumatori un miglior controllo sui dati GPS.
- Molte aziende che sviluppano app si trovano fuori dell'Europa, per cui non sono vincolate dalle normative europee sulla protezione dei dati personali. È quindi difficile per l'Unione Europea insistere sul fatto che le app debbano essere rispettose della privacy. Tuttavia un recente emendamento della direttiva sulla privacy elettronica insiste sul fatto che gli utenti devono poter dare il loro consenso all'elaborazione di dati provenienti dalle app installate sui loro smartphone, indipendentemente da dove si trovi nel mondo la sede del fornitore delle app.
- Analogamente al DPI, nei paesi dove un governo nazionale e le aziende di telefonia mobile hanno un rapporto stretto, le informazioni potrebbero essere condivise in un modo che dia allo Stato l'accesso ai dati di geolocalizzazione di tutti i cittadini.

9 Biometria

Il termine 'biometria' può riferirsi a sistemi che utilizzano caratteristiche fisiologiche misurabili di una persona - come impronte digitali, DNA, retina, struttura facciale, odori corporei - oppure all'analisi di tratti comportamentali unici della persona, come l'analisi dell'andatura e dell'impronta vocale e lo stile di battitura sulla tastiera, allo scopo di riconoscere l'identità, verificare l'identità presunta di un individuo o classificarlo.



Alcuni paesi rilevano le impronte digitali e altri identificatori biometrici dei loro cittadini e li archiviano in carte di identità nazionali o in un database. A questo punto le caratteristiche di una persona vengono accolte e memorizzate in un sistema biometrico. Successivamente i dati biometrici della persona vengono confrontati con le informazioni archiviate al momento del "reclutamento", cioè dell'inserimento nel database, per verificare l'identità di quella persona. Significativi progressi in campo informatico hanno portato a sistemi biometrici automatizzati, che permettono, ad esempio, controlli di massa dell'identità nel giro di pochi secondi.

9.1 Perché è stata sviluppata la biometria

Nell'Ottocento lo sviluppo dei sistemi giudiziari nazionali richiese un modo più formale per identificare le persone. Questi sistemi cercavano di trattare meno pesantemente chi commetteva un reato per la prima volta e più duramente i criminali recidivi. Occorreva quindi un sistema formale che regi-

strasse i reati insieme a caratteri identificativi misurati del colpevole. In Francia, Alphonse Bertillon sviluppò il "Bertillonage" o antropometria, un metodo di identificazione delle persone basato sulla registrazione dettagliata delle loro misure corporee, come altezza o lunghezza delle braccia, descrizioni fisiche e foto. Intorno al 1890 emerse un approccio più promettente: Sir Francis Galton riuscì a sviluppare un metodo per reperire le registrazioni che consentivano di individuare i criminali sulla base delle impronte digitali, un identificatore più personalizzato rispetto alle misurazioni di Bertillon. Nel XX secolo furono scoperti altri potenziali identificatori biometrici. Nel 1936 Frank Burch propose di utilizzare gli schemi dell'iride come mezzo di riconoscimento di un individuo, e nel 1960 furono sviluppate tecniche di riconoscimento facciale e vocale.

9.2 Come viene usata la biometria

Tradizionalmente la biometria viene usata dalle forze dell'ordine per individuare criminali noti e sconosciuti o per autorizzare l'accesso a luoghi sicuri, edifici governativi, strutture industriali ecc.

Nel XXI secolo la biometria viene sempre più utilizzata nel contesto della sicurezza delle frontiere. Vengono rilevati i dati biometrici dei visitatori che chiedono un visto per visitare uno specifico paese. All'arrivo questi dati biometrici vengono controllati con un database per verificare, ad esempio, se un viaggiatore è stato precedentemente dichiarato "inammissibile", costituisce notoriamente un rischio per la sicurezza o ha precedentemente soggiornato nel Paese oltre la scadenza del visto. La UE, ad esempio, raccoglie anche 10 impronte digitali e una foto digitale delle persone che chiedono un visto UE. Questi dati biometrici vengono archiviati nel database VIS (VISA Information System). Analogamente, la UE ha istituito EURODAC (Dattiloscopia Europea), un grande database di impronte digitali dei richiedenti asilo e dei migranti trovati privi di documenti all'interno della UE. Il database aiuta l'applicazione effettiva della Convenzione di Dublino, relativa alla gestione delle richieste di asilo politico.

In ambito militare, le forze armate statunitensi hanno impiegato, sui campi di battaglia in Afghanistan e in Iraq, dispositivi mobili per sottoporre di routine le persone da loro incontrate a scansioni dell'iride o ad altre scansioni biometriche. Le persone oggetto di interesse sono state successivamente inserite in un 'Elenco di controllo biometrico', che permette ai soldati sul campo di verificare l'identità di un sospetto terrorista o di rivelare che un individuo del posto ha legami con una rete insurrezionale e che quindi non può essere impiegato presso una base militare USA fuori degli Stati Uniti. Il database contiene finora 209.000 registrazioni di individui in tutto il mondo.

Anche se originariamente la biometria può essere stata creata per identificare persone a fini di sicurezza, nell'arco del XX secolo è stata sempre più utilizzata per sviluppare meccanismi commerciali di controllo dell'accesso. Il suo vantaggio è che, a differenza di chiavi e password, i tratti personali

sono estremamente difficili da perdere o dimenticare e molto difficili da copiare. Per questo motivo, molti li ritengono più sicuri di chiavi o password. I nuovi iPhone della Apple, ad esempio, hanno adesso un sensore di impronta digitale che è in grado di effettuare la scansione del dito dell'utente. Facebook utilizza strumenti di riconoscimento facciale per suggerire automaticamente l'identità di una persona in una foto. Il suo progetto di ricerca, DeepFace, è in grado di dire, con un grado di precisione del 97,25%, se due foto contengono lo stesso volto. Le banche stanno sviluppando la biometria vocale per consentire ai clienti di accedere ad una carta di credito ed effettuare pagamenti sul cellulare semplicemente pronunciando una frase d'accesso. Le aziende utilizzano computer portatili con lettore di impronte digitali integrato per il controllo biometrico dell'accesso. Gli schermi pubblicitari sulle strade possono anche mostrare pubblicità diverse a seconda della persona che li sta guar-

Come funziona l'identificazione biometrica

Il primo passo consiste nell'ottenere dall'individuo il campione biometrico, ad esempio un'impronta digitale o una scansione dell'iride, tipicamente mediante una foto. I dati possono essere archiviati come foto o come *template*, ovvero come rappresentazione digitale dei dati biometrici creata usando un algoritmo. Per tutelare la privacy al meglio sarebbe opportuno archiviare solo il *template*, eliminando l'immagine originaria.

I dati biometrici, cioè la foto o il *template*, possono essere archiviati in varie posizioni, ad esempio nel centro operativo in cui è avvenuto il 'reclutamento' (ad esempio in un lettore) per essere utilizzati successivamente, e su un dispositivo trasportato dall'individuo (ad esempio su una smart card). Potrebbero anche essere inviati e archiviati in un database centralizzato accessibile da uno o più sistemi biometrici.

Quando si accede ad un sistema biometrico, esso chiede alla persona di presentare le caratteristiche biometriche. Il sistema confronterà poi la foto o il *template* del campione presentato con i dati biometrici della persona registrati nel sistema.

Se il processo di 'abbinamento' biometrico riesce, il sistema riconosce e accetta la persona. Se l'abbinamento non riesce, la persona non viene riconosciuta e di conseguenza viene 'rifiutata'. La foto o il *template* creati quando i dati biometrici sono stati registrati per la prima volta raramente sono identici alla foto o al *template* delle caratteristiche biometriche che vengono presentati successivamente. La caratteristica in oggetto spesso cambia lievemente o viene presentata in modo leggermente diverso rispetto al momento dell'inserimento nel database. Nell'abbinamento esiste quindi inevitabilmente un certo grado di incertezza.

La biometria può essere usata anche nella prevenzione dei reati, specialmente quando viene impiegata l'analisi di tratti del comportamento personale e lo scopo non è l'identificazione di uno specifico individuo ma la sua classificazione. Il riconoscimento facciale e le funzioni di analisi comportamentale delle TVCC possono essere considerati come funzioni biometriche.

dando, sulla base dell'età o del sesso.

I dati biometrici, tuttavia, vengono sempre più utilizzati non solo come strumenti di identificazione, ma di analisi comportamentale. Numerose app relative al fitness utilizzano dati biometrici in tempo reale, come la frequenza cardiaca e la frequenza respiratoria, per fornire raccomandazioni su misura per gli utenti della app. Nel campo della sicurezza, nuove capacità di elaborazione biometrica vengono aggiunte ad un sistema preesistente (ad esempio riconoscimento facciale nelle TVCC), ottenendo nuove capacità di sorveglianza. In questo contesto è importante notare che i nuovi sistemi biometrici sono potenzialmente in grado di raccogliere informazioni a distanza o in movimento senza la necessità di collaborazione o azione da parte dell'individuo. Tali sistemi potrebbero far scattare un allarme, ad esempio quando una TVCC identifica un criminale noto la cui immagine sia stata memorizzata in un database della polizia.

9.3 Miglioramenti della sicurezza

La biometria può migliorare la sicurezza nei seguenti modi.

- L'identificazione mediante elementi biometrici viene usata da più di 100 anni dalle forze dell'ordine per compiti di verifica e di identificazione. I sistemi che analizzano il volto di una persona, come pure i sistemi che ne analizzano il DNA, possono contribuire molto efficacemente alla lotta contro il crimine e rivelano in modo efficiente l'identità di una persona sconosciuta sospettata di un grave reato.
- La raccolta di dati biometrici può essere utilizzata per aumentare la sicurezza di specifiche attività di elaborazione di dati sensibili. Può aiutare, ad esempio, a garantire che solo persone autorizzate presso lo specifico operatore telefonico abbiano accesso a dati di traffico (e a dati di localizzazione) che devono essere conservati a fini di applicazione della legge.

9.4 Problematiche

Occorre considerare numerosi aspetti negativi.

1. I dati biometrici non sono infallibili.

- Possiamo dire che due registrazioni digitali di un tratto biometrico non sono mai esattamente identiche. Differenze nel tipo di attrezzatura utilizzata al momento dell'inserimento nel database o differenze ambientali (luce, temperatura) possono causare false percentuali di accettazione e di rifiuto: un sistema biometrico può identificare in modo errato un individuo oppure non rifiutare un impostore (falso tasso di accettazione). Si ha un 'falso rifiuto' quando un individuo non viene abbinato al proprio *template* biometrico esistente.
 - Le caratteristiche biometriche della persona, inoltre, possono cambiare durante la sua vita, ad esempio a causa di invecchiamento, intervento chirurgico o incidente. Un sistema biometrico potrebbe non riconoscerla più.
 - Sono possibili falsificazioni dei dati biometrici, e ciò aumenta la possibilità di un furto d'identità.
 - Allo stato attuale della tecnologia è ancora molto facile ingannare, ad esempio, un sistema biometrico di riconoscimento facciale apportando semplici modifiche nell'aspetto, come un differente taglio di capelli, barba, trucco, occhiali, lenti a contatto ecc.
2. In passato l'uso della biometria era costoso e richiedeva molto tempo. A causa di queste limitazioni, l'impatto sui diritti di protezione dei dati personali era ridotto. Tutto questo è cambiato, e potrebbe portare alla discriminazione genetica e alla graduale perdita di privacy se non verranno adottate misure di salvaguardia appropriate. Ad esempio, equipaggiare i sistemi di video-sorveglianza e gli smartphone con sistemi di riconoscimento facciale basati sui database dei social network potrebbe porre fine all'anonimato e alla libertà di movimento dei singoli individui.
 3. Nella maggior parte dei casi l'inserimento nel database richiede il coinvolgimento personale del singolo, ad esempio nel caso delle impronte digitali, e può quindi fornire una valida opportunità per dare informazioni e comunicare in modo equo la proce-

dura. Tuttavia è possibile anche 'reclutare' gli individui senza la loro conoscenza o il loro consenso, ad esempio utilizzando sistemi TVCC con funzionalità di riconoscimento facciale incorporata. Ciò ha gravi conseguenze sulla loro capacità di esercitare il libero consenso o semplicemente di ottenere informazioni sull'elaborazione di questi dati.

4. La biometria intesa come caratteristiche inalterabili può inoltre essere problematica se ci sono stati errori nella fase di inserimento nel database, con potenziale erronea stigmatizzazione di un individuo.

10 La tecnologia basata sulla sorveglianza è l'unica risposta?

Lei potrebbe benissimo chiedersi se le tecnologie per la sicurezza siano l'unica soluzione ai problemi di sicurezza. A volte sembra che la sicurezza consista solo nel rintracciare e identificare sospetti all'interno della popolazione generale. Le tecnologie per la sicurezza orientate alla sorveglianza operano nel presupposto che un sistema di sorveglianza esteso che monitori quante più persone possibile nel modo più accurato possibile sia il modo migliore per individuare potenziali azioni pericolose e identificare potenziali criminali dopo che il reato è stato commesso, o, in alternativa, anche prima che esso venga effettivamente commesso. Ogni volta che vengono implementate tecnologie di questo tipo, la sicurezza viene ricercata quasi esclusivamente aumentando la sorveglianza.

In parte è vero, ma le cose non stanno solo così. Mentre le tecnologie per la sicurezza vengono usate per scoprire criminali e terroristi e prevedere le loro prossime mosse, esistono strategie diverse che puntano ad aumentare la sicurezza attraverso altri mezzi. In questo capitolo esemplificheremo alcuni approcci che possono essere considerati come misure di sicurezza alternative.

Dal punto di vista sociale, 'sicurezza' è un termine ambiguo, che può essere recepito in modi diversi. Il livello di sicurezza percepito è fortemente collegato a condizioni quali la stabilità sociale, la certezza o l'affidabilità sociale, per citarne solo alcune.

10.1 Misure di sicurezza alternative: il livello globale

Le priorità europee relative alla sicurezza, che abbiamo esaminato in precedenza, sembravano suggerire che la sicurezza sia qualcosa che riguarda tutti gli ambiti della vita. Essa riguarda le questioni 'classiche' come la criminalità e il terrorismo. Da ciò che abbiamo visto nelle pagine precedenti, è possibile usare le nuove tecnologie della sicurezza per trovare gli individui coinvolti in tali attività. Alla radice di questi problemi di sicurezza, tuttavia, si trovano cause, come la povertà, i conflitti nazionali o internazionali, oppure le differenze politiche e religiose. Le tecnologie per la sicurezza non sono in grado di affrontare queste "cause ultime".

Le priorità europee relative alla sicurezza includono tra i problemi di sicurezza anche le crisi o le calamità naturali. Può trattarsi di mancanza di cibo o di acqua, crisi finanziarie, diffusione di malattie o calamità naturali: tutte cose che mettono a rischio la sicurezza umana nel suo complesso. Se pensiamo alla sicurezza in termini di "sicurezza complessiva del genere umano", può essere utile dare un breve sguardo ad alcune delle sfide globali che la società deve affrontare.

È possibile, in qualche misura, proporre e attuare iniziative di sicurezza che puntino ad accrescere il livello di sicurezza relativo alle catastrofi naturali o causate dall'uomo. Tali iniziative si radicano molto spesso in approcci globali a lungo termine. La promozione di sistemi globali di commercio equo-solidale, aiuto e cancellazione del debito, ad esempio, cerca di affrontare non solo questioni economiche, ma anche le questioni ambientali connesse all'eccessivo sfruttamento delle risorse naturali, all'inquinamento e a gravi alterazioni dei cicli ambientali e climatici. Queste sono, in definitiva, questioni di sicurezza. Allo stesso modo, le politiche che puntano a migliorare le risposte a catastrofi locali e nazionali, o le politiche volte a migliorare le infrastrutture informatiche e di comunicazione e le forniture di cibo e acqua, sono anch'esse modi alternativi per migliorare le condizioni di vita e ottenere così migliori livelli di sicurezza nelle aree in oggetto.

Modi diversi di intendere la sicurezza, e quindi modi diversi di promuovere la sicurezza, sono stati sviluppati non solo a livello globale. Vorremmo quindi richiamare la Sua attenzione sul Suo ambiente locale, per individuare tutta una serie di ulteriori approcci che cercano di potenziare la sicurezza.

In sintesi: soluzioni nazionali e internazionali

- Promuovere sistemi globali di commercio equo e solidale, aiuti e allentamento del debito;
- Promuovere politiche economiche e sociali orientate a una più equa distribuzione di redditi e impiego;

- Migliorare le infrastrutture e le risorse destinate a rispondere alle calamità;
- Usare più efficacemente fonti di energia sostenibili e alternative;
- Migliorare le infrastrutture idriche, di comunicazione e informatiche, e fornire aiuti alimentari nelle parti del mondo dove ne esiste la necessità.

10.2 Misure di sicurezza alternative: il livello locale

Esistono modi diversi e alternativi di intendere e perseguire maggiori livelli di sicurezza a livello locale. Si può, ad esempio, perseguire la sicurezza implementando tecnologie che non comportino sorveglianza. Metal detector, luci sensibili al movimento, allarmi volumetrici, dispositivi di allarme generici o anche telefoni pubblici di emergenza sono tutte tecnologie che puntano ad aumentare la sicurezza senza introdurre la sorveglianza o il reperimento dati. Esse cercano invece di aumentare la capacità degli individui di reagire e intervenire per proteggere se stessi e le loro proprietà. In alternativa, tecnologie come i metal detector aiutano le autorità pubbliche a scoprire potenziali pericoli focalizzandosi sulla sorgente della minaccia (l'oggetto metallico) anziché sulle caratteristiche dell'individuo che potenzialmente costituisce un pericolo. La loro efficacia può essere molto alta, ma limitata allo specifico momento e allo specifico luogo in cui esse sono in azione. Non costituiscono tuttavia una minaccia in termini di privacy o di sorveglianza.

Tentativi di prevenire i reati e aumentare la sicurezza negli spazi pubblici possono essere effettuati anche attraverso la gestione e la pianificazione urbanistica. Modifiche strutturali volte a promuovere un ambiente urbano più sicuro, ad esempio riducendo le zone pericolose (in strade, piazze, parchi difficili da tenere sotto osservazione), possono prima di tutto aiutare ad accrescere il livello di sicurezza percepita nella sfera pubblica e, contemporaneamente, aiutare i cittadini ad essere più consapevoli dell'ambiente che li circonda e dei pericoli che potrebbero presentarsi.

In sintesi: approcci non basati sulla sorveglianza e sulla raccolta di dati

- Prevenzione dei reati attraverso la pianificazione urbanistica e il design ambientale;
- Implementazione di tecnologie che non comportano sorveglianza.

È possibile anche introdurre misure di sicurezza che perseguono l'aumento dei livelli di sicurezza grazie alla sorveglianza ma non prevedono necessariamente tecnologie che portano ad una massiccia raccolta e archiviazione di dati. Un esempio tipico potrebbe essere costituito dal rafforzamento delle attività di polizia, come l'aumento delle pattuglie di polizia locale. Le attività di polizia tradizionali, in effetti, perseguono anch'esse l'aumento del livello di sicurezza attraverso una sorveglianza non tecnologica. Esistono inoltre i programmi di "ronde di quartiere", che funzionano ridistribuendo le attività di pattugliamento tra i vicini di aree residenziali, che controllano le attività sospette nelle loro aree e le riferiscono alla polizia locale. I controlli d'identità attraverso l'utilizzo di elenchi precompilati di ospiti allo scopo di regolare l'accesso in luoghi privati o pubblici, redatti da portieri o personale di sicurezza, sono anch'essi esempi di misure di sicurezza che si basano sulla sorveglianza per aumentare la sicurezza ma non coinvolgono tecnologie o reperimento massiccio di dati.

In sintesi: approcci per aumentare la sorveglianza non basati sulle tecnologie

- Rafforzamento delle attività di polizia tradizionali;
- Attuazione di programmi di 'ronde di quartiere' e simili;
- Impiego di personale di sorveglianza, cioè personale di sicurezza o portieri.

Esistono infine modi di garantire la sicurezza che perseguono livelli di sicurezza più elevati non tanto attraverso la repressione delle attività criminali o la minaccia della deterrenza, ma piuttosto attraverso un nuovo approccio globale a lungo termine capace di affrontare le cause socioeconomiche che sono alla base della violenza, del crimine, dell'odio religioso, del razzismo o della discriminazione sociale. Anche in questo caso le tecnologie per la sicurezza sono meno efficaci nell'affrontare questi

problemi di sicurezza 'umani' più complessi e a lungo termine.

Sulla base di questa concezione più ampia della sicurezza, sono state proposte varie misure politiche, come la creazione di migliori rapporti della comunità locale con la polizia o il coinvolgimento di gruppi religiosi o altri gruppi comunitari nella gestione dei problemi locali allo scopo di aumentare la fiducia e la coesione sociale. In definitiva, le opzioni di sicurezza sono rappresentate anche dall'incremento del livello di sostegno sociale ed economico grazie a politiche attive di occupazione, ad opportunità di formazione e tutoraggio per coloro che rischiano di essere coinvolti in reati. Anche le associazioni di volontariato per la riabilitazione di alcolisti o tossicodipendenti, la realizzazione di centri di accoglienza per migranti o l'istituzione di centri sociali spesso autogestiti sono ulteriori esempi di misure locali che cercano di aumentare la coesione sociale migliorando contemporaneamente i livelli di sicurezza in una data zona.



L'idea che sta alla base di questi approcci alla sicurezza è di duplice natura: da un lato riguarda la partecipazione attiva delle persone interessate (= i cittadini locali) nella soluzione del conflitto, e dall'altra punta anche a reintegrare malviventi o colpevoli attraverso un lavoro comunitario sociale anziché attraverso punizioni disciplinari.

Politiche scolastiche attive, orientate all'integrazione, all'autogestione e al rispetto della diversità, possono contribuire a ridurre le tensioni sociali, culturali ed economiche e a migliorare il senso di appartenenza alle comunità locali e nazionali, con-

tribuendo così indirettamente ad accrescere i livelli di sicurezza.

In sintesi, approcci riguardanti le condizioni sociali e la 'mitigazione' a lungo termine:

- Investire in mezzi, misure e personale sociali;
- Favorire la partecipazione attiva dei cittadini nella soluzione di questioni e conflitti locali;
- Stabilire migliori relazioni comunitarie all'interno dei vari gruppi interessati;
- Aumentare il supporto (economico) per politiche dell'occupazione, opportunità di formazione ecc.;
- Realizzare centri di accoglienza, centri di quartiere, centri sociali.

In questo capitolo abbiamo presentato brevemente approcci e concezioni alternative, ma anche in questo caso Lei potrebbe avere idee diverse su come migliorare la sicurezza. O forse Lei ritiene che il focus della sicurezza europea dovrebbe spostarsi dalla criminalità e dal terrorismo e concentrarsi su altre priorità.

11 Ora tocca a Lei...

Lei è arrivato alla fine dell'opuscolo e può prendersi un po' di tempo per riflettere sulle questioni sollevate in queste pagine.

Abbiamo descritto le cinque tecnologie per la sicurezza di cui parleremo durante il focus group. Abbiamo spiegato come funzionano, come vengono utilizzate, i miglioramenti che offrono per la sicurezza e le questioni che sollevano. Abbiamo anche spiegato il contesto in cui queste tecnologie si sono sviluppate: in un'Europa che è molto preoccupata della sicurezza e dove la sicurezza fa parte della vita quotidiana. Sono importanti anche le questioni della sorveglianza e della privacy, vista la quantità di dati personali che attualmente vengono impiegati nel contesto della sicurezza. Abbiamo infine accennato ad approcci alternativi, non tecnologici, per garantire la sicurezza nella società.

Tocca ora a Lei riflettere su ciò che pensa di questi temi. Se queste tecnologie venissero usate di routine a fini di sicurezza, sarebbero accettabili? Può darsi che Lei ritenga che ciascuna di esse è a suo modo efficace nell'aumentare la sicurezza e ridurre potenzialmente la criminalità. Ma potrebbe anche ritenere che sarebbe meglio adottare soluzioni alternative, non tecnologiche. Forse Lei pensa che dovrebbero essere usati metodi più tradizionali, come personale di vigilanza e forze dell'ordine adeguatamente addestrati, anziché una sorveglianza estesa sulle informazioni. Forse Lei pensa che la sicurezza non sia in realtà un problema e che non ce ne dovremmo preoccupare troppo.

Analogamente, forse Lei è fiducioso che queste tecnologie siano in mani sicure perché utilizzate da

istituzioni pubbliche che devono rispondere ai cittadini. O forse Lei ha dei dubbi sulla capacità di tali istituzioni di utilizzare le tecnologie per la sicurezza in modo competente, etico, avendo a cuore gli interessi di ciascun componente della società.

Forse Lei ritiene che le tecnologie in realtà non la riguardino: dopotutto, hanno per obiettivo altri che hanno commesso reati e vengono usate in spazi o luoghi dove Lei non va. O invece potrebbe ritenere che chiunque dovrebbe interessarsi della questione, vista la quantità di dati elaborati dalle tecnologie e il fatto che esse rendono chiunque un potenziale sospetto. Forse Lei va bene come vengono usate attualmente le tecnologie per la sicurezza, ma è preoccupato per come potranno essere utilizzate in futuro.

Qualunque cosa Lei creda, barattare un po' di privacy per un po' più di sicurezza non è una decisione semplice per nessuno. SurPRISE intende capire la gamma di opinioni espresse dalla gente riguardo alle nuove tecnologie per la sicurezza.

Ci auguriamo di vederla all'evento partecipativo tra poche settimane. Se vuole saperne di più sul progetto e sui suoi partner, La invitiamo a visitare il sito web del focus group italiano www.eui.eu/surprise o quello del progetto SurPRISE <http://surprise-project.eu>.

‘I problemi legati alla privacy sono questioni politiche, non solo questioni legali e tecnologiche.’

Colin J. Bennet, docente ed esperto di sicurezza presso il Dipartimento di Scienze Politiche della University of Victoria, Canada.

Questo documento

Questo opuscolo è stato realizzato per informare i cittadini che prenderanno parte ai focus group del progetto SurPRISE. La diffusione di questo documento a tutti i partner del consorzio SurPRISE è a cura dell'Istituto di valutazione delle tecnologie (Accademia Austriaca delle Scienze, Strohgassee 45/5, A-1030 Vienna). Maggiori informazioni sul progetto e sui partner sono reperibili nel sito web <http://surprise-project.eu>.

Le informazioni contenute in questo libretto provengono da report scritti da membri del progetto SurPRISE, che a loro volta hanno attinto alla ricerca e ai report scritti da scienziati, politici e tecnologi di tutto il mondo.

Questo opuscolo è una versione estesa e rivista dell'opuscolo informativo scritto dalla dott.ssa Kirstie Ball (The Open University) nel 2013 per gli eventi partecipativi su larga scala che si sono tenuti in nove paesi europei nei primi tre mesi del 2014.

- Autori: dott.ssa Kirstie Ball, The Open University; Maria Grazia Porcedda e Mathias Vermeulen, EUI; Elvira Santiago and Vincenzo Pavone, CSIC; Regina Berglez, IRKS; Eva Schlehahn, ULD; Márta Szénay, Medián
- Comitato scientifico consultivo: Dott.ssa Monica Areñas Ramiro, Robin Bayley, Prof. Colin Bennett, Dott.ssa Gloria González Fuster, Dott. Ben Hayes, Dott. Majtényi László, Jean Marc Suchier, Nina Tranø, Prof. Ole Wæver
- Layout: Zsolt Bartha, Medián, rivisto a partire da quello del primo opuscolo informativo preparato da Peter Devine, David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University
- Immagini: David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University. pagina 12: Vision Systems, <http://www.visionsystems.co.nz/assets/Vid-eo-Analytics1.jpg> pagina 16 Mat Wellington, "Police Use QuadCopter – UK" March 23rd 2011, <http://multirotor-news.com/2011/03/23/police-use-quadcopter-uk> pagina 20 © iStock-Photo.com / alexsl, pagina 21 Senseable City Lab, Massachusetts Institute of Technology page 24 © KIVI NIRIA DV, 2011
- Il progetto SurPRISE è finanziato dal Settimo programma quadro di ricerca dell'Unione Europea in base all'accordo di assegnazione numero 285492.
- Questa pubblicazione è disponibile al sito: <http://surprise-project.eu>.

Partners di progetto

- Institut für Technikfolgen-Abschätzung/Osterreichische Akademie der Wissenschaften, Coordinator, Austria (ITA/OEAW)
- Agencia de Protección de Datos de la Comunidad de Madrid*, Spain (APDCM)
- Instituto de Políticas y Bienes Públicos/Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain (CSIC)
- Teknologiradet - The Danish Board of Technology Foundation, Denmark (DBT)
- European University Institute, Italy (EUI)
- Verein für Rechts-und Kriminalsoziologie, Austria (IRKS)
- Median Opinion and Market Research Limited Company, Hungary (Median)
- Teknologiradet - The Norwegian Board of Technology, Norway (NBT)
- The Open University, United Kingdom (OU)
- TA-SWISS/Akademien der Wissenschaften Schweiz, Switzerland (TA-SWISS)
- Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein/Germany (ULD)

* APDCM, the Agencia de Protección de Datos de la Comunidad de Madrid (Autorità garante per la protezione dei dati personali della Comunità di Madrid) è stata membro del progetto SurPRISE fino al 31 dicembre 2012. APDCM è stata soppressa a causa delle politiche di austerità adottate in Spagna.

Questo progetto è finanziato dal Settimo Programma Quadro di ricerca dell'Unione Europea in base all'accordo di assegnazione numero 285492.

Sorveglianza, Privacy e Sicurezza: uno studio partecipativo su larga scala dei criteri e fattori che determinano l'accettabilità e l'accettazione delle tecnologie di sicurezza in Europa.

