



Sorveglianza, Privacy e Sicurezza

QUAL È LA TUA OPINIONE?



surprise

surveillance
privacy
security



Indice

1	Benvenuti a SURPRISE	5
	1.1 Come leggere questo opuscolo	6
2	Riepilogo	7
3	Un giorno qualunque...	9
	3.1 Sorveglianza, privacy e sicurezza	10
	3.1.1 Sorveglianza	10
	3.1.2 Privacy e protezione dei dati: questioni importanti?	11
	3.1.3 Sicurezza	12
4	Tre nuove tecnologie per la sicurezza	13
5	Cybersorveglianza mediante Deep Packet Inspection (DPI)	15
	5.1 Perché è stato messo a punto il DPI	15
	5.2 Come viene usato il DPI	16
	5.2.1 Usi commerciali	17
	5.2.2 Impieghi per la sicurezza pubblica e nazionale	18
	5.3 Miglioramenti della sicurezza	19
	5.4 Problematiche	19
6	Geolocalizzazione degli smartphone	21
	6.1 Perché è stata sviluppata la geolocalizzazione degli smartphone	21
	6.2 Come viene usata la geolocalizzazione degli smartphone	23
	6.2.1 Usi commerciali	23
	6.2.2 Impieghi per la sicurezza pubblica e nazionale	24
	6.3 Miglioramenti della sicurezza	24
	6.4 Problematiche	25
7	TVCC smart	27
	7.1 Perché è stata messa a punto la TVCC smart	27
	7.2 Come viene usata la TVCC smart	29
	7.3 Miglioramenti relativi alla sicurezza	30
	7.4 Problematiche	30
8	La tecnologia è l'unica risposta?	33
	8.1 Soluzioni locali	33
	8.2 Soluzioni nazionali o internazionali	33
9	Ora tocca a Lei...	35
	Questo documento	36

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 essere fatto per garantire la loro sicurezza. Partecipando all'evento partecipativo SurPRISE Lei potrà condividere il suo punto di vista sulle nuove tecnologie per la sicurezza con altri cittadini. SurPRISE raccoglierà i pareri dei cittadini su queste nuove tecnologie e li condividerà con la Commissione Europea.

Gli eventi partecipativi si svolgono in nove paesi europei: Gran Bretagna, Austria, Danimarca, Germania, Ungheria, Italia, Norvegia, Spagna e Svizzera. I risultati degli eventi partecipativi verranno consegnati all'Unione Europea entro

l'estate del 2014. Saranno inoltre resi pubblici e messi a disposizione dei mezzi di comunicazione, dei governi e dei cittadini.

Questo opuscolo fornisce informazioni di base sui temi che verranno discussi durante l'evento partecipativo SurPRISE italiano a febbraio 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.

Sappiamo che leggere questo testo potrebbe essere impegnativo per Lei, ma la nostra intenzione non è di valutare le Sue attuali conoscenze, né di fare di Lei un esperto! Lo scopo dell'opuscolo è di darle un'idea dei temi che verranno discussi durante l'evento partecipativo e permetterle di cominciare a riflettere su qual è la Sua personale opinione riguardo a sorveglianza, privacy e sicurezza. La Sua partecipazione all'evento 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.

SurPRISE fornirà ai rappresentanti eletti e ad altri decisori le opinioni dei cittadini raccolte in modo anonimo. Le tecnologie per la sicurezza fanno riferimento ai diritti umani, a questioni di giustizia ed equità, all'efficacia e all'affidabilità delle istituzioni. Ecco perché i dibattiti dovrebbero coinvolgere tutta la cittadinanza, non solo i politici, le industrie, gli esperti e le organizzazioni umanitarie. 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!**

1.1 Come leggere questo opuscolo

La prossima sezione offre un riepilogo degli argomenti successivamente trattati in maggiore dettaglio nel testo. Dopo il riepilogo, l'opuscolo si articola in cinque capitoli principali. Il primo è un'introduzione generale ai temi della sorveglianza, della sicurezza e della privacy in Europa. I capitoli successivi descrivono le tecnologie per la sicurezza di cui parleremo durante l'evento partecipativo. Anche se l'opuscolo si occupa di tre tecnologie, all'evento ne discuteremo solo due. La Sua lettera d'invito Le dirà quali tecnologie saranno oggetto dell'evento partecipativo.

Ciascun capitolo descrive perché è stata sviluppata la tecnologia, come viene utilizzata, i miglioramenti nella sicurezza che essa offre e i suoi limiti. All'interno di ciascun capitolo abbiamo inserito un box informativo che spiega più in dettaglio il funzionamento di quella specifica tecnologia, e un box che descrive un aspetto controverso di tale tecnologia. Il capitolo finale esamina brevemente alcune alternative alle tecnologie per la sicurezza.

Se non desidera leggere l'intero documento, legga il riepilogo, che contiene una sintesi dei punti principali.

2 Riepilogo

L'obiettivo di SurPRISE è quello di capire che cosa pensano i cittadini europei delle nuove tecnologie per la sicurezza. Sempre più preoccupati per il terrorismo, la criminalità organizzata e i reati informatici, i governi europei stanno investendo nello sviluppo di nuove tecnologie per la sicurezza. Molte di queste tecnologie analizzano le informazioni generate dai cittadini nella 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.

Poiché queste tecnologie utilizzano dati personali, le chiamiamo "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.

Durante l'evento partecipativo SurPRISE esamineremo approfonditamente due di queste tre tecnologie:

- > **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 cellulare 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.
- > **TVCC smart:** impianti di videosorveglianza a circuito chiuso che vanno al di là del sem-

plice 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.

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, ad esempio, funziona solo in determinate condizioni e può 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. Il mancato controllo sulla raccolta e sull'utilizzo delle informazioni è una questione legata a tutte le tecnologie oggetto del nostro esame.

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?
- > Possiamo fidarci dell'uso che ne fanno le istituzioni?
- > Esiste una regolamentazione giuridica sufficientemente efficace?
- > Chi sorveglia i sorveglianti?
- > Quali sono le alternative, e sono praticabili?

Queste sono alcune delle questioni che discuteremo durante l'evento partecipativo.

Continui a leggere per maggiori dettagli su questi temi.

3 Un giorno qualunque...

Appena a sud di Budapest, Marta prende la E-75, la strada europea che porta all'aeroporto internazionale di Ferihegy. Ripensa alla prima volta che l'ha attraversata. Allora pagava il pedaggio al casello: ora il pedaggio viene addebitato automaticamente sul suo conto corrente bancario. La targa della sua auto viene letta da delle telecamere di riconoscimento automatico delle targhe e il sistema di pagamento del pedaggio fa il resto. Prima Marta non si era mai accorta delle telecamere sospese in alto. Ora le vede e si chiede come fanno a collegarsi alla sua banca.

Marta parcheggia l'auto e sale sullo shuttle che la porta al terminal. Lì fa il check in utilizzando l'apposita macchinetta self-service. Appoggia il passaporto sulla macchina che confronta il suo nome con i dati della prenotazione. Quando Marta riceve la sua carta d'imbarco, si rende conto che anche in questo caso i suoi dati personali sono memorizzati da qualche parte.

Una volta passati i controlli sicurezza, Marta va al bar e appoggia in terra il suo bagaglio a mano. Ordina un caffè, ma di nuovo si ferma prima di porgere la carta di debito al cassiere. "Molto comoda la plastica", pensa, "ma chi registra questa operazione e perché?"

Mentre beve il caffè, Marta tira fuori lo smartphone per controllare i messaggi. Quando lo schermo si accende, la geolocalizzazione visualizzata sulla schermata Home cambia immediatamente da "Kecskemét", dove Marta vive, a "Ferihegy". Come ha fatto a saperlo? Deve esistere una spiegazione assolutamente ovvia, ma non riesce a immaginarla.

Marta ha appena il tempo di inviare un'e-mail a una collega di lavoro prima di salire a bordo dell'aereo. Quando mette il suo telefono in modalità Flight, si chiede che cosa accadrà alla sua e-mail nel percorso attraverso Internet.

La vicenda di Marta non è insolita, è comune a tutti i viaggiatori. Le tecnologie offrono a Marta dei vantaggi nel senso che rendono il suo viaggio più comodo ed efficiente, tuttavia suscitano in lei anche delle domande: "Chi usa i miei dati personali, e che cosa significa per me che questi dati sono 'nel sistema'?"

Molte delle tecnologie incontrate da Marta sono presenti anche al di fuori del mondo aeroportuale. Moltissima gente non riuscirebbe a immaginare la propria vita senza smartphone, carte di debito o Internet! Di fatto, molte attività quotidiane generano il tipo di traccia elettronica di cui Marta sta diventando consapevole. Forse anche Lei ha in mente le stesse domande. 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. Forse Marta è preoccupata proprio di questo, ma allo stesso tempo è anche combattuta, perché queste tecnologie offrono effettivamente dei vantaggi.

Tecnologie come quelle esaminate sopra, e i dati da esse raccolti, possono offrire vantaggi 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 tecnologie 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.

Se Marta considerasse che i suoi dati potrebbero essere usati in questo modo, sarebbe ancora preoccupata? Se ciò significasse maggiore sicurezza per lei e per chiunque altro, forse sarebbe qualcosa che lei potrebbe accettare. Tuttavia 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.

Sorgono altre domande:

- > Possiamo fidarci delle istituzioni che utilizzano i dati?
- > Tali istituzioni sono ben regolamentate?
- > Le tecnologie vengono utilizzate in modo conforme alla legge?
- > Le istituzioni sono trasparenti e rispondono di eventuali violazioni della privacy commesse in nome della sicurezza?
- > Tali tecnologie migliorano realmente la sicurezza?

Queste sono alcune delle domande che prenderemo in esame durante l'evento partecipativo.

Nei prossimi paragrafi presenteremo alcuni dei termini e definizioni chiave prima di descrivere tre nuove tecnologie per la sicurezza, due delle quali verranno trattate durante l'evento partecipativo.

3.1 Sorveglianza, privacy e sicurezza

3.1.1 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 per individuare i malviventi in strada. La sorveglianza può avere anche scopi commerciali: un supermercato potrebbe, ad esempio, usare le tessere fedeltà per capire che cosa preferiscono comprare

gruppi diversi di consumatori. Ciò influirà su quali offerte speciali verranno proposte in futuro a tali clienti. 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.

3.1.2 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.

3.1.3 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 opinioni diverse su ciò che costituisce una minaccia per la sicurezza e su ciò che sarebbe disposto a fare per proteggere le cose che ritiene importanti.

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 naturale.

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, come Airbus, BEA Systems e Finmeccanica, 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 Tre nuove tecnologie per la sicurezza

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

- > **Cybersorveglianza tramite DPI**
- > **Geolocalizzazione degli smartphone**
- > **TVCC smart**

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 l'evento partecipativo 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 Cybersorveglianza mediante Deep Packet Inspection (DPI)

Seduta al bar dell'aeroporto, Marta si chiedeva che cosa sarebbe successo alla e-mail inviata alla sua collega durante il viaggio attraverso Internet. Forse si sarebbe imbattuta in una tecnica di cybersorveglianza denominata DPI (deep packet inspection, ispezione approfondita – o filtraggio - dei pacchetti di dati).

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 leggere il 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. 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 lavorano per scoprire e configurare il modo in cui i messaggi viaggiano su una rete. Esse aprono e analizzano 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.



5.1 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.

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 avviene nei 'router'. Il router è un computer che indirizza i messaggi sulle varie reti che compongono Internet. Tutte le apparecchiature nei 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. Sono le società che possiedono i router, quelle che per prime hanno realizzato la tecnologia che esegue il DPI. Naturalmente le società intendono usare la tecnologia per i propri 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.

5.2 Come viene usato il DPI

In Europa il DPI può essere usato legalmente solo in misura molto limitata. Secondo le leggi esistenti, può essere usata 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. Anche là dove è consentita, non può essere usata indiscriminatamente. La legge europea sulla tutela della privacy e la Carta dei diritti fondamentali dell’Unione Europea 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 (programmi denominati rispettivamente Upstream e Tempora), 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. I sistemi DPI generano nuove informazioni, che possono a loro volta essere

condivise tra i fornitori di servizi internet ed i governi, ed è difficile conoscere il destino dei risultati delle ricerche effettuate tramite DPI. 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. Ci sono alcuni usi noti del DPI al di là delle ampie attività di sorveglianza delle agenzie di sicurezza statunitensi rivelate l’estate scorsa: alcuni sono commerciali, altri si riferiscono alla sicurezza pubblica e nazionale.

5.2.1 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 consentita, 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.

Controversia sul DPI: Phorm e dati dei consumatori in Gran Bretagna

Nel 2008 l'azienda statunitense Phorm ha cercato di lanciare in Gran Bretagna un sistema insieme ai fornitori di telecomunicazioni British Telecom, Virgin Media e TalkTalk. Phorm ha usato il DPI per intercettare le abitudini di navigazione web degli utenti mentre essi stavano appunto navigando. Ha poi analizzato i dati prima di venderli alle società pubblicitarie. I fornitori hanno detto agli utenti che tali misure combattevano la criminalità informatica, ma non hanno rivelato che stavano usando i dati a fini pubblicitari. British Telecom ha condotto sperimentazioni segrete sulla tecnologia, effettuando più di 18 milioni di intercettazioni. I consumatori britannici lo hanno scoperto e hanno protestato perché i dati erano stati elaborati senza il loro consenso. Alla fine la tecnologia Phorm è stata abbandonata da tutti i fornitori. La Commissione Europea ha poi fatto causa al governo britannico, che aveva permesso il funzionamento di tale servizio. Il caso è stato chiuso nel gennaio 2012, dopo che la Gran Bretagna ha emendato le proprie leggi includendo una sanzione per l'intercettazione illegale di comunicazioni.

5.2.2 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 in Europa Internet venga censurato.

5.3 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.

- > 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.

5.4 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 raffreddamento", 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.

3. È difficile localizzare esattamente chi sta usando il DPI e dove.

- > Le norme giuridiche dovrebbero essere uguali in tutto il mondo. Da qualche tempo le autorità garanti della privacy in tutto il mondo stanno chiedendo uno standard minimo internazionale di privacy.
- > Un "regolamentatore" del DPI dovrebbe essere un ente veramente internazionale con potere sufficiente a punire i trasgressori.

4. L'efficacia del DPI è discutibile:

- > 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.



“Molte delle società che utilizzano il DPI si trovano fuori dall'Europa ma analizzano dati relativi ai cittadini europei. Per questo motivo non si può dire loro di non analizzarli”.

Eva Schlehan, Garante per la protezione dei dati personali, Schleswig Holstein (Germania)

6 Geolocalizzazione degli smartphone

Quando Marta ha acceso il suo smartphone, ha notato che la schermata iniziale indicava che il luogo dove si trovava era cambiato. Lei era certa che dietro tutto questo ci fosse una spiegazione logica. In effetti, tutti i tipi di cellulare hanno bisogno di sapere dove si trovano per poter funzionare. Gli smartphone hanno portato questa esigenza a un livello completamente nuovo.

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.

6.1 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. Come si ricorderà, a metà degli anni Novanta cominciò ad apparire un numero molto più alto di antenne. Ci furono molti dibattiti pubblici sul posizionamento di tali orribili antenne e preoccupazioni sanitarie sull'aumento dei livelli di radiazione.

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. 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.

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.

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, cercò di ottenere le registrazioni dei dati di geolocalizzazione del suo cellulare relativi ai sei mesi precedenti, dovette citare in giudizio l'azienda telefonica per ottenerle. Una volta ricevuti i dati, 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 - Stati Uniti contro Jones - 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".

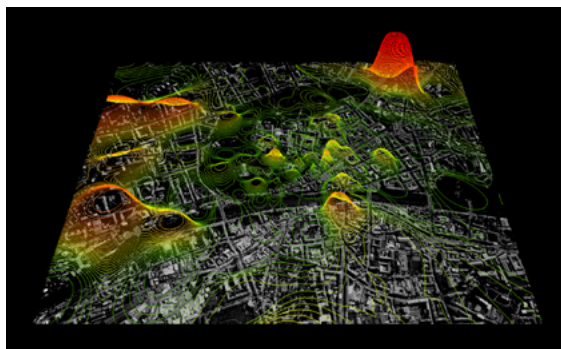
6.2 Come viene usata la geolocalizzazione degli smartphone

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

6.2.1 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.

6.2.2 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 continuativamente) 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'.

6.3 Miglioramenti della sicurezza

La geolocalizzazione degli smartphone migliora la sicurezza in vari modi:

1. Permette di trovare e aiutare persone in situazioni di pericolo;
2. Permette alle famiglie di tenere sotto controllo adulti vulnerabili o bambini;
3. 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.

6.4 Problematiche

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

1. 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.
2. Alcune 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.
3. 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.
4. 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.
5. Poiché i dati GPS sono stati usati per identificare i partecipanti alle proteste, il loro uso ha un potenziale 'effetto raffreddamento', in quanto gli individui possono diventare cauti e limitare le proteste e l'esercizio dei loro diritti democratici.



“La geolocalizzazione degli smartphone offre molto alle persone, ma allo stesso tempo le sorveglia. Può fornire molti servizi e migliorare i rapporti sociali... ma la condivisione dei dati GPS non è sempre così ovvia o facile da gestire...”

Gus Hosein, Privacy International

7 TVCC smart

Abbiamo visto come Marta, nel suo viaggio verso l'aeroporto, si chiedeva come funzionassero le telecamere che le addebitavano il pedaggio. Erano telecamere per la lettura e il riconoscimento automatico delle targhe, ovvero telecamere ANPR, che costituiscono un esempio della nuova tecnologia per la sicurezza denominata 'TVCC smart', cioè impianto di videosorveglianza a circuito chiuso digitale 'intelligente'.

La maggior parte degli europei conosce bene gli impianti di videosorveglianza a circuito chiuso. 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.



7.1 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 statunitensi e britanniche negli anni Sessanta. L'uso della TVCC è cresciuto costantemente in tutta Europa negli anni Novanta, soprattutto in Gran Bretagna, seguita a breve distanza da Francia e Olanda. È sempre stata al centro dell'attenzione mediatica. Nel 2013 gli impianti TVCC sono stati determinanti per individuare i responsabili delle bombe alla maratona di Boston.

La TVCC smart 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 impianto 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.

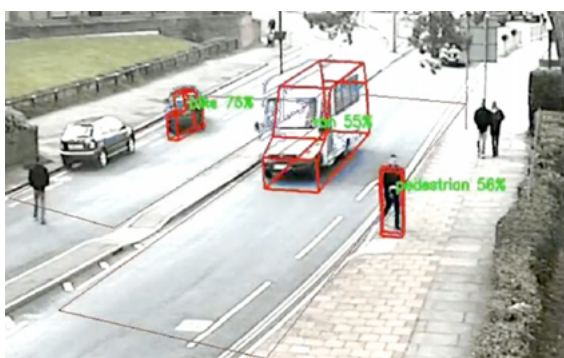
Il software della TVCC smart può fare molte cose. Perlopiù viene usato per::

- > 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.

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', '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.

7.2 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.

A Budapest alla fine del 2012 la polizia ha iniziato a usare telecamere smart per monitorare le corsie preferenziali degli autobus. La polizia può usare le immagini legalmente, purché non vengano filmati i passeggeri e la cittadinanza sia perfettamente informata. Telecamere con riconoscimento facciale sono state installate nell'aeroporto di Zurigo nel 2003. All'epoca fu il primo utilizzo del riconoscimento facciale nel contesto dei controlli alle frontiere. Questo impianto è ormai installato permanentemente.

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 meritino lo stesso tipo di sorveglianza. La TVCC smart dovrebbe essere usata per tutti i tipi di reato 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 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. In Gran Bretagna il sistema ANPR è stato usato per il pagamento del pedaggio a Londra, e ora è integrato nelle strategie della polizia sia nazionale che locale. A partire dal 2010 sono state installate in Gran Bretagna 500 telecamere ANPR, e il centro dati nazionale della polizia legge fra i 10 e i 14 milioni di registrazioni ANPR al giorno.

Controversia sulla TVCC smart: ANPR a Birmingham (GB)

Nel 2011 la polizia di Birmingham ha dovuto rimuovere telecamere ANPR da tre zone della città densamente popolate da residenti di religione musulmana. Le telecamere erano state finanziate nel quadro di un programma antiterrorismo denominato "Project Champion", ma erano state pubblicizzate al pubblico come strumenti per la sicurezza. I leader della comunità e i parlamentari locali si sono opposti con forza alle telecamere e i rapporti all'interno della popolazione ne hanno risentito. 200 telecamere sono state installate ma non sono mai state accese. 64 telecamere erano nascoste ed erano state installate senza aver consultato la popolazione. Le telecamere sono state distrutte oppure utilizzate da altre forze di polizia britanniche. Il fallimento del progetto e la perdita delle telecamere sono costati alla polizia 300.000 sterline (equivalenti a 351.814 euro).

7.3 Miglioramenti relativi alla sicurezza

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

1. 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.
2. 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.

7.4 Problematiche

Occorre tener presenti numerosi svantaggi della TVCC smart.

1. 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.
2. 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.
3. 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.



“Occorre trasparenza: dobbiamo spiegare perché abbiamo installato impianti TVCC smart. Le persone dovrebbero poter contattare il responsabile dell'impianto per chiedere informazioni sul suo utilizzo. Esse hanno bisogno di convincersi che la telecamera è lì per un valido motivo, e hanno bisogno di aver fiducia nel suo corretto utilizzo”.

Chris Tomlinson, Consulente per la sicurezza

8 La tecnologia 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. In parte è vero, ma le cose non stanno solo così.

Le priorità europee relative alla sicurezza, che abbiamo esaminato sopra, 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. Ancora una volta, le tecnologie per la sicurezza sono meno efficaci nell'affrontare questi problemi di sicurezza a più lungo termine, più complessi.

Tali tecnologie vengono dunque utilizzate per scoprire criminali e terroristi e spiare le loro prossime mosse, ma esistono anche altre soluzioni. Sotto ne abbiamo elencate alcune. Forse Lei ha qualche idea personale su come potrebbe essere migliorata la sicurezza. O forse Lei ritiene che il focus della sicurezza europea dovrebbe spostarsi dalla criminalità e dal terrorismo e concentrarsi su altre priorità.

8.1 Soluzioni locali

- > Promuovere la sicurezza dell'ambiente urbano, grazie ad una migliore illuminazione delle strade, a telefoni pubblici di emergenza e a una maggiore presenza della polizia.
- > Stabilire migliori rapporti tra ente locale e polizia, attraverso interventi di prevenzione della criminalità da parte di tale ente.
- > Fare in modo che i gruppi religiosi o altri gruppi comunitari gestiscano i problemi localmente, in modo da aumentare il livello di fiducia sociale.
- > Avere amministratori locali e politici locali trasparenti e affidabili.
- > Offrire molte opportunità di lavoro, di formazione e di accompagnamento a coloro che rischiano di essere reclutati dalla criminalità.

8.2 Soluzioni nazionali o internazionali

- > Promuovere sistemi globali di commercio equo e solidale, aiuti e allentamento del debito.
- > Migliorare le infrastrutture e le risorse destinate a rispondere alle calamità.
- > Migliorare le infrastrutture idriche, di comunicazione e informatiche, e fornire aiuti alimentari nelle parti del mondo dove ne esiste la necessità.
- > Usare più efficacemente fonti di energia sostenibili e alternative.
- > Risolvere i problemi di disuguaglianza e discriminazione.

9 Ora tocca a Lei...

Ci auguriamo di non averla confusa con un eccesso di informazioni! La buona notizia è che Lei è arrivato alla fine del libretto e può prendersi un po' di tempo per riflettere sulle questioni che abbiamo sollevato.

Abbiamo descritto le tecnologie per la sicurezza di cui parleremo durante l'evento partecipativo. 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 dell'evento partecipativo SurPRISE: **www.eui.eu/surprise**.

Questo documento

Questo opuscolo è stato realizzato per informare i cittadini che prenderanno parte agli eventi partecipativi 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.

- > Autore: dott.ssa Kirstie Ball, The Open University
- > 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: 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
- > Sponsors SurPRISE: Settimo programma quadro (FP7) della Commissione Europea
- > Questa pubblicazione è disponibile nel sito: <http://surprise-project.eu>
- > Com'è stato prodotto il documento. Questo opuscolo informativo è stato scritto da Kirstie Ball in stretta collaborazione con il Danish Board of Technology Foundation, con il consorzio SurPRISE ed il suo Comitato consultivo. Il libretto è stato sottoposto a quattro passaggi di revisione interna, uno di revisione esterna ed è stato poi testato con gruppi in Danimarca, Ungheria e Gran Bretagna.

Partners di progetto

- > Institut für Technikfolgen-Abschätzung / Österreichische Akademie der Wissenschaften
Coordinator, Austria
- > 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
- > Teknologirådet - The Danish Board of Technology Foundation, Denmark
- > European University Institute, Italy
- > Verein für Rechts-und Kriminalsoziologie, Austria
- > Median Opinion and Market Research Limited Company, Hungary
- > Teknologirådet - The Norwegian Board of Technology, Norway
- > The Open University, United Kingdom
- > TA-SWISS / Akademien der Wissenschaften Schweiz, Switzerland
- > Unabhängiges Landeszentrum für Datenschutz, Germany

•APDCM, l'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.

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



