European University Institute
DEPARTMENT OF LAW

surprise

"Surveillance, Privacy and Security:
A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe"

Risultati preliminari dell'evento partecipativo italiano

SurPRISE "Uno studio partecipativo su larga scala dei criteri e fattori che determinano l'accettabilità e l'accettazione delle tecnologie di sicurezza in Europa."

Progetto Cooperativo
FP7 Call Topic SEC-2011.6.5-2: The Relationship Between Human Privacy And Security
Inizio del progetto: febbraio 2012; Durata: 36 mesi

Autrici: Maria Grazia Porcedda e Melissa Zorzi
Contatti: maria.porcedda@eui.eu e melissa.zorzi@eui.eu

Seventh
Framework Programme
of the European Union

Questo documento è stato redatto dal progetto SurPRISE (http://www.surprise-project.eu), un progetto cofinanziato dal Settimo Programma Quadro (FP7). SurPRISE rimette in discussione la relazione tra sicurezza e privacy. SurPRISE fornirà una nuova analisi sulla relazione tra sorveglianza, privacy e sicurezza, partendo dalla prospettiva dei cittadini. Inoltre esplorerà la possiiblità di usare tecnologie di sicurezza alternative a quelle che violano la privacy e soluzioni di sicurezza non orientate alla sorveglianza, generando così un dibattito più informato sulle politiche di sicurezza. Il progetto SurPRISE è condotto da un consorzio costituito dai seguenti membri:

InstitutfürTechnikfolgen-Abschätzung / Oesterreichische Akademie derWissenschaften Coordinator, Austria	ITA/OEAW	
Agencia de Protección de Datos de la Comunidad de Madrid,[1] Spagna	APDCM	
Instituto de Politicas y BienesPublicos/ AgenciaEstatalConsejoSuperiorde InvestigacionesCientíficas, Spagna	CSIC	
Teknologirådet - The DanishBoard of Technology Foundation, Denmark	DBT	
European University Institute, Italia	EUI	
VereinfürRechts-und Kriminalsoziologie, Austria	IRKS	
Median Opinion and Market Research Limited Company, Ungheria	Median	
Teknologirådet - The NorwegianBoard of Technology, Norvegia	NBT	
The Open University, Regno Unito	OU	
TA-SWISS / AkademienderWissenschaftenSchweiz, Svizzera	TA-SWISS	
UnabhängigesLandeszentrumfürDatenschutz, Germania	ULD	

Questo documento può essere liberamente usato e distribuito, a patto che il documento medesimo non sia modificato o abbreviato, che sia dato piano riconoscimento ai suoi autori, e che queste condizioni non siano rimosse, ma anzi incluse in ogni copia. I partners del progetto SurPRISE non sono in alcun modo responsabili per la completezza, adeguatezza e appropriatezza dell'uso. Questo documento potrebbe essere sottoposto ad aggiornamenti, emendamenti e aggiunte da parte del consorzio SurPRISE. La preghiamo di rivolgere eventuali domande e commenti a: feedback@surprise-project.eu.

[1] APDCM, the Agencia de Protección de Datos de la Comunidad de Madrid (Agenzia di Protezione dei dati della Comunità di Madrid) è stata membro del consorzio SurPRISE fino al 31 decembre 2012, quando è statasoppressa in conseguenza delle politiche di austerità in Spagna

Indice

1 Il progetto SurPRISE e l'Italia

SurPRISE è un progetto europeo di ricerca co-finanziato dal Settimo Programa Quadro della Commissione Europea. Il nome è l'acronimo inglese di "Sorveglianza, privacy, sicurezza",[2] mentre il titolo completo è: "Uno studio partecipativo su larga scala dei criteri e fattori che determinano l'accettabilità e l'accettazione delle tecnologie di sicurezza in Europa."[3] L'obiettivo principale di SurPRISE è, infatti, quello di capire che cosa pensano i cittadini europei delle nuove tecnologie per la sicurezza che analizzano le informazioni generate dai cittadini nella vita quotidiana: le "tecnologie per la sicurezza orientate alla sorveglianza".[4]

La fase chiave del progetto consiste nella realizzazione di una consultazione pubblica[5] con i cittadini dei nove paesi europei partecipanti: Austria, Danimarca, Germania, Italia, Norvegia, Spagna, Regno Unito, Ungheria e Svizzera. Il partner italiano del progetto SurPRISE è l'Istituto Universitario Europeo, che ha organizzato la consultazione pubblica per l'Italia a Firenze. Fino ad ora, oltre all'Italia, 5 dei paesi europei coinvolti hanno svolto eventi partecipativi. Gli eventi ad Aarhus (Danimarca) del 18 gennaio, a Budapest (Ungheria) del 25 gennaio, a Oslo (Norvegia) e a Madrid (Spagna) del 1 febbraio e a Vienna (Austria) del 22 febbraio hanno già dato dei risultati interessanti.

I 2000 partecipanti europei sono invitati a discutere dell'impiego a scopo di sicurezza di due tra le seguenti tecnologie: geolocalizzazione tramite smartphone e cellulari, sistemi di videosorveglianza intelligenti e *deep packet inspection* (DPI, una delle tecnologie usate nell'ambito del datagate). Le consultazioni pubbliche offrono ai cittadini l'occasione di riflettere ed esprimere il proprio punto di vista e di redigere raccomandazioni riguardo alle questioni sollevate dall'utilizzo da parte degli Stati europei di queste nuove tecnologie. Tra le problematiche discusse si possono elencare le seguenti: l'efficacia delle tecnologie nel garantire una maggiore sicurezza, l'accettabilità di forme di sorveglianza nella vita quotidiana, la relazione tra l'utilizzo delle tecnologie e il diritto alla riservatezza e alla protezione dei dati personali, la regolamentazione dell'utilizzo delle tecnologie e la fiducia nelle istituzioni che le impiegano.

[2] "Surveillance, privacy, security. A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe".

[3] Maggiori informazioni sul progetto sono reperibili al sito (in inglese): www.surprise-project.eu.

[4] Definita come "una tecnologia che utilizza informazioni raccolte in vari contesti e relative alla popolazione generale e alle sue attività allo scopo di affrontare un problema riguardante la sicurezza." Il materiale informativo sarà pubblicato alla pagina: www.eui.eu/surprise.

[5] Affine a quelle previste in Toscana dalla Legge regionale 46/2013 Dibattito pubblico regionale e promozione della partecipazione alla elaborazione delle politiche regionali e locali, Bollettino Ufficiale n. 39, parte prima, del 7 agosto 2013 (preceduta per il periodo 2007-2012 dalla Legge 69/2007 Norme sulla promozione della partecipazione alla elaborazione delle politiche regionali e locali, Bollettino Ufficiale n. 1, parte prima, del 3 gennaio 2008.

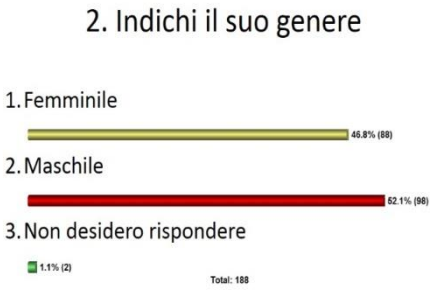
2 L'evento partecipativo italiano: Firenze, 8 febbraio 2014

Coerentemente con quanto previsto dal progetto, l'Istituto Universitario Europeo ha organizzato l'evento italiano, che si è svolto l'8 febbraio 2014 a Firenze[6] presso il Palazzo degli Affari del complesso Firenze Fiera, con il patrocinio della Regione Toscana, della Provincia di Firenze, del Comune di Firenze, del Forum Italiano per la Sicurezza Urbana, del Garante per la protezione dei dati personali e della Rappresentanza in Italia della Commissione Europea.

La giornata si è aperta con la presentazione del progetto da parte del professor Martin Scheinin, direttore scientifico del progetto SurPRISE all'Istituto Universitario Europeo, e con il saluto di benvenuto dell'Assessore del Comune di Firenze Cristina Giachi. L'evento è stato condotto dal dott. Paolo Martinez (FUTOUR). I partecipanti italiani hanno discusso e deliberato sull'impiego, da parte delle istituzioni preposte alla sicurezza, della cybersorveglianza tramite *deep packet inspection* (DPI) e della geolocalizzazione degli smartphone.

2.1 193 cittadini a confronto[7]

All'evento hanno preso parte 193 cittadini provenienti da diversi comuni della provincia di Firenze: Bagno a Ripoli, Dicomano, Empoli, Firenze, Fiesole, Fucecchio, Scandicci, Scarperia e Vaglia. Come illustrato dal seguente grafico, il campione era ben bilanciato per genere (47% femmine e 53% maschi) ed età (la stessa quota di partecipanti di età inferiore e superiore ai 50 anni).



La maggioranza (ca. 60%) è stata campionata[8] in quanto rappresentativa della popolazione residente nella provincia di Firenze sulla base dei seguenti criteri demografici: genere, età, titolo di studio, professione, luogo di residenza (rurale/cittadino), luogo di origine (regione dell'Italia).
I cittadini invitati, estratti casualmente dalle liste dell'anagrafe dei comuni coinvolti, sono stati reclutati tramite chiamata telefonica e lettera inviata per posta ordinaria o elettronica. L'8% dei partecipanti è stato reclutato a catena attraverso altri partecipanti già reclutati, mentre un altro 8% si è autocandidato in risposta ai manifesti affissi a Firenze nel mese di gennaio. Il rimanente 23% dei partecipanti appartiene a

[6] Maggiori informazioni sull'evento italiano sono reperibili alla pagina: www.eui.eu/surprise.

[7] Questo evento non sarebbe stato possibile senza l'appoggio e l'apporto di numerose persone. Grazie a: Serena Bürgisser, vicedirettrice dell'Ufficio Stampa, Giulia Serafini e Michele Massacesi; Paolo Martinez (FUTOUR); l'Assessore Cristina Giachi, per il suo saluto di benvenuto, e tutti gli enti pubblici che ci hanno concesso il patrocinio morale (Regione Toscana, Provincia di Firenze, Comune di Firenze, Forum Italiano per la Sicurezza Urbana, Garante per la protezione dei dati personali e Rappresentanza in Italia della Commissione Europea); Jonathan Andrew (team SURVEILLE), Claudia De Concini (team SURVEILLE/SurPRISE), Martyn Egan (EUI) e Matteo Rocchi (assistenza durante l'evento); Rete e Sviluppo s.c. e lo studio Baglioni e Poponcini (campionamento e reclutamento); i moderatori e segretari ai tavoli: Ginevra Avalle, Fabio Baglioni, Francesca Bonechi, Sandro Buggiani, Nicolò Caciotti, Francesca Casini, Luca Caterino, Lorenzo Cecchi, Lapo Cecconi, Riccardo Emilio Chesta, Carmelo Chianura, Giulia Ciampi, Paola Cimbolli, Céline Colombo, Federica Coppola, Marco Algimiro Fusaro, Stefania Gatti, Katia Giannone, Dario Miccoli, Valentina Miola, Sofie Christine Møller, Davide Morisi, Eleonora Moscardi, Vanna Mugnaini, Alfredo Panerai, Fausto Petrini, Silvia Poponcini, Francesco Ranghiasci, Laura Remaschi, Francesco Renzetti, Emanuele Rigutto, Filippo Salvucci, Marco Scarselli, Grazia Sciacchitano, Veronica Spada, Annalisa Suman, Teresa Talò, Gloria Vitaioli, Antonio Volino e Alberto Zinanni.

[8] Il campionamento e reclutamento è stato eseguito da reteSviluppo s.c. (http://www.retesviluppo.it/).

minoranze (ad es. stranieri comunitari e non comunitari residenti in provincia di Firenze e diversamente abili), ed è stato reclutato tramite associazioni presenti sul territorio.[9]

2.2 La metodologia del Danish Board of Technology

Il Danish Board of Technology, partner danese del consorzio SurPRISE, ha condiviso con il progetto la propria lunga esperienza nell'organizzazione di eventi partecipativi, sviluppando la metodologia e le linee guida per lo svolgimento di tutti gli eventi partecipativi. La metodologia, simile a quella dei Town Meeting, prevede che i partecipanti ricevano tutti lo stesso livello di informazione (attraverso un opuscolo informativo e di sostegno alla discussione, inviato ai partecipanti due settimane prima dell'evento, e la proiezione di documentari durante l'evento) e che prendano parte ai lavori divisi in tavoli di discussione, ciascuno guidato da un moderatore. I 193 cittadini che hanno partecipato all'evento italiano sono stati divisi in 35 tavoli.

La giornata di lavoro è stata organizzata in tre sessioni: due tematiche relative alle tecnologie trattate all'evento italiano (la cybersorveglianza tramite DPI e la geolocalizzazione degli smartphone) e una dedicata alla deliberazione e alle raccomandazioni dei cittadini. Durante le sessioni tematiche i partecipanti hanno guardato un documentario (realizzato dal consorzio SurPRISE) sulla tecnologia in discussione, hanno espresso la loro opinione tramite un sistema di voto elettronico remoto con proiezione immediata dei risultati, e hanno discusso del tema ai tavoli. Durante la terza sessione, i partecipanti di ciascun tavolo hanno redatto insieme una raccomandazione destinata a politici e istituzioni nazionali ed europee; alcuni tavoli sono stati poi invitati a leggere le loro raccomandazioni. Infine, i partecipanti hanno risposto ad alcune domande di carattere generale sulla percezione della sicurezza, la fiducia nelle istituzioni, l'impatto delle tecnologie della sorveglianza sulla privacy e sulla necessità di utilizzare delle alternative.

2.3 Questo documento

Questo documento presenta i risultati preliminari delle votazioni e delle raccomandazioni, cui farà seguito un report nazionale completo che sarà pubblicato in primavera. Nella prossima sezione riportiamo alcuni interessanti risultati delle votazioni in merito a sicurezza, tecnologie orientate alla sorveglianza e privacy in Italia. Nella quarta sezione presentiamo alcuni risultati salienti delle sessioni tematiche dell'evento. Nella quinta e ultima sezione offriamo una sintesi delle raccomandazioni dei partecipanti.

***

La relazione dei risultati comparati dei nove eventi partecipativi svolti in Europa sarà pubblicata a inizio estate. A giugno il progetto SurPRISE organizzerà dei focus group in cinque dei paesi coinvolti nel progetto, tra cui l'Italia, sull'uso dei droni a scopo di sicurezza. I risultati generali degli eventi partecipativi e dei focus groups saranno presentati all'Istituto Universitario Europeo a ottobre.

[9] Il reclutamento è stato eseguito dalla ditta Baglioni & Poponcini (http://www.baglionipoponcini.it/).

3 Sicurezza, tecnologie della sorveglianza e privacy in Italia: una questione di fiducia

All'inizio e alla fine della giornata i partecipanti hanno risposto ad alcune domande di carattere generale sulla percezione della sicurezza, la fiducia nelle istituzioni, l'impatto delle tecnologie della sorveglianza sulla privacy e sulla necessità di utilizzare delle alternative. Qui riportiamo alcuni risultati a confronto.

Sicurezza

Il 43% dei partecipanti pensa che l'Italia sia un paese sicuro in cui vivere e il 38% si sente al sicuro nella vita quotidiana. È notevole, però, che il 29% e il 39% rispettivamente non esprimano una posizione netta (né d'accordo né in disaccordo) sulla sensazione di sicurezza.

Conoscenza delle tecnologie orientate alla sorveglianza e uso a scopo di sicurezza nazionale

Prima della visione del documentario e della discussione ai tavoli, il 51,6% dei cittadini ha dichiarato di essere d'accordo con l'utilizzo delle tecnologie per la sicurezza orientate alla sorveglianza per migliorare la sicurezza nazionale, pur esprimendo, nel 79% dei casi, una conoscenza pregressa molto limitata sulle tecnologie stesse. Dopo la discussione sul DPI e la geolocalizzazione degli smartphone e la visione dei filmati correlati, la conoscenza limitata sulle tecnologie era espressa solo dal 39% dei partecipanti, mentre il 79,6% si è detto d'accordo con l'affermazione "l'uso delle tecnologie per la sicurezza orientate alla sorveglianza migliora la sicurezza nazionale."

Impatto sulla privacy dell'uso delle tecnologie

Prima della visione del documentario e della discussione ai tavoli, poco più della metà dei partecipanti ha espresso il timore che le tecnologie per la sicurezza orientate alla sorveglianza potessero mettere a rischio la protezione della loro privacy (54% dei voti) e la privacy come diritto (60% dei voti). Alla fine della giornata dei lavori il 66% era preoccupato per la propria privacy, e il 72% per la privacy in quanto diritto fondamentale. Nello specifico, il 63% dei partecipanti si è detto preoccupato che vengano raccolte troppe informazioni personali e ben l'89,7% ha espresso il timore che i propri dati personali possano essere condivisi senza autorizzazione.

Nonostante il fatto che il 77,8% dei cittadini abbia espresso la preoccupazione che i dati personali raccolti possano essere usati contro di loro, sarebbe riduttivo ricondurre la preoccupazione per la privacy a una dimensione strettamente individuale. Come descritto sopra, infatti, i partecipanti hanno espresso uguale preoccupazione per la privacy sia a livello individuale sia collettivo. Inoltre, la votazione sul quesito "Se non si fa niente di male, non si deve essere preoccupati per le tecnologie per la sicurezza orientate alla sorveglianza" ha mostrato una distribuzione omogenea dei voti (d'accordo il 30%, in disaccordo il 26%), indicando anche che i cittadini non sono pronti a pagare un'accresciuta sicurezza con la perdita del loro diritto alla privacy.

***

Da quest'analisi preliminare sembra emergere un paradosso: da un lato i cittadini approvano l'utilizzo da parte degli organismi di sicurezza di tecnologie orientate alla sorveglianza, dall'altro esprimono preoccupazione per le ripercussioni negative sul diritto alla riservatezza e alla protezione dei dati personali. La chiave di lettura potrebbe trovarsi nella votazione sul quesito: "Una volta che vengono installate delle tecnologie per la sicurezza orientate alla sorveglianza, è probabile che si verifichino abusi nel loro utilizzo", con cui l'82% dei partecipanti è d'accordo.

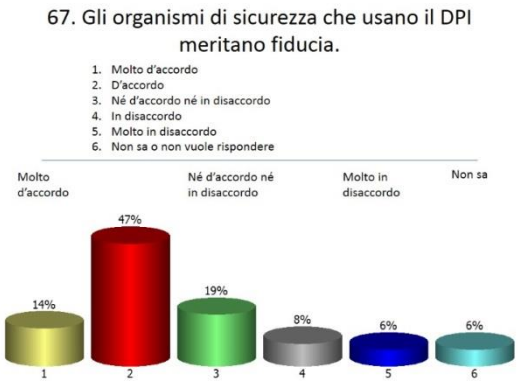
Per quanto riguarda la proposta di soluzioni, la percentuale dei partecipanti che darebbe priorità maggiore ad approcci alternativi alla sicurezza che non coinvolgano tecnologie orientate alla sorveglianza è calata dal 72% al 66% nel corso della giornata, un dato per il quale sarà necessaria un'analisi approfondita delle raccomandazioni proposte dai cittadini.

4 Sessioni tematiche: *Deep Packet Inspection* e geolocalizzazione degli smartphone

4.1 Uso del DPI a scopo di sicurezza: intrusività e fiducia

La prima sessione tematica dell'evento italiano riguardava la cybersorveglianza tramite *Deep Packet Inspection* (filtraggio dei pacchetti di dati che transitano sul web), che consiste nell'uso di dispositivi hardware e di un software specifico per leggere, analizzare e modificare tutti i messaggi e le informazioni trasmessi su Internet. Innanzitutto, la stragrande maggioranza dei partecipanti usa spesso o sempre Internet (79%), mentre l'8% non lo usa mai. Oltre la metà dei partecipanti (56%) è preoccupato della sicurezza quando è connesso (mentre il 23% non si preoccupa, e il 5% non sa o non vuole rispondere).

Se nel complesso il 55% dei cittadini appoggia l'adozione del DPI come misura di sicurezza nazionale (e al contrario il 19% si oppone), tale consenso non è incondizionato. Le statistiche riportate qui di seguito mostrano che oltre il 60% dei partecipanti ritiene che gli organismi di sicurezza che usano il DPI meritino fiducia (con un 19% di indecisi), tuttavia il 43,17% teme che quegli stessi organismi possano abusare del loro potere. Pesa la mancanza d'informazioni specifiche sulle modalità d'impiego delle tecnologie: il 44% dei partecipanti esprime incertezza sulla competenza degli organismi di sicurezza nelll'uso delle medesime.



Il timore espresso dev'essere messo in relazione con la preoccupazione, manifestata dall'83% dei partecipanti, che il DPI possa violare i diritti fondamentali di chiunque (il tasso di preoccupazione per una violazione dei propri diritti è sostanzialmente uguale); lo scandalo del datagate potrebbe aver avuto un peso nella formazione della percezione dei partecipanti. Nello specifico della privacy, il 74% teme che il

DPI possa rivelare dati sensibili individuali e ben il 77% teme che il DPI possa violare la confidenzialità delle comunicazioni.

Da notare come il 72% dei partecipanti sia preoccupato per i futuri sviluppi dell'uso del DPI.

4.2 Uso della geolocalizzazione degli smartphone a scopo di sicurezza: intrusività e fiducia

La seconda sessione tematica dell'evento italiano ha riguardato la geolocalizzazione degli smartphone e dei cellulari. Possono essere localizzati sia i cellulari "normali" sia i cellulari "smart" ed esistono tre modi per tracciare un cellulare: attraverso antenne telefoniche, sistemi di posizionamento globale (GPS) o reti wireless. La prima modalità vale per tutti i cellulari, mentre la seconda e la terza si applicano solo agli smartphone. Analizzando i dati di posizione provenienti da un cellulare è possibile raccogliere informazioni sulla localizzazione e sui movimenti di un utente telefonico in un determinato arco di tempo.

L'80,2% dei cittadini presenti ha dichiarato di usare spesso o sempre dispositivi mobili come cellulari o smartphone, mentre il 4,9% ha dichiarato di non usarli mai.

Sebbene nel complesso il 70,6% dei cittadini appoggi l'adozione della geolocalizzazione degli smartphone come misura di sicurezza nazionale (e al contrario 12,2% si opponga), l'utilizzo per scopi di sicurezza di questa tecnologia non è privo di rischi per i cittadini. I grafici riportati di seguito mostrano che il 59,5% dei partecipanti ritiene che gli organismi di sicurezza che usano la geolocalizzazione degli smartphone meritino fiducia (con un 23,2% di indecisi), tuttavia il 31% teme che gli stessi organismi di sicurezza possano abusare del loro potere e il 42% non riesce a prendere una posizione sul quesito. Come nel caso del DPI, probabilmente pesa la mancanza di informazioni specifiche sulle modalità d'impiego delle tecnologie. Nel caso della geolocalizzazione degli smartphone, il 39% dei partecipanti esprime incertezza sulla competenza degli organismi di sicurezza nelll'uso delle medesime.

Il timore espresso va messo in relazione con la preoccupazione, manifestata dal 69,4% dei partecipanti, che la geolocalizzazione degli smartphone possa violare i diritti fondamentali di chiunque (il tasso di preoccupazione per una violazione dei propri diritti fondamentali è leggermente inferiore, 63%). Nello specifico della privacy, il 55,4% teme che la geolocalizzazione possa rivelare dati sensibili individuali, il 72,8% teme che la geolocalizzazione possa dare adito a un'interpretazione errata del proprio comportamento e il 66% dei cittadini teme che la geolocalizzazione possa far conoscere a estranei la propria posizione.

Infine, nel 53% dei casi i partecipanti sono preoccupati per i futuri sviluppi della geolocalizzazione degli smartphone, in misura quindi inferiore rispetto al DPI.

5 Le raccomandazioni dei cittadini

Dopo le sessioni tematiche, i cittadini hanno redatto, presso ciascun tavolo di lavoro, una raccomandazione, destinata alle autorità e ai politici nazionali ed europei, sull'impiego delle tecnologie per la sicurezza orientate alla sorveglianza. Tutti e 35 i tavoli hanno indirizzato la loro raccomandazione a un'istituzione pubblica, in alcuni casi a livello nazionale, in altri a livello europeo e in altri ancora a livello internazionale.

Le azioni suggerite si possono raggruppare sotto 5 capitoli:

I. Regolamentazione

I cittadini domandano l'adozione di una normativa efficace per disciplinare l'impiego dei dati personali raccolti attraverso le nuove tecnologie a fini di sicurezza o a fini commerciali. I cittadini hanno espresso, in particolare, la necessità di una maggiore armonizzazione delle leggi dei paesi membri dell'Unione europea o di una normativa uniforme a livello europeo che 'segua' i dati, proteggendoli, anche quando vengono trattati al di fuori dei confini dell'Unione, come nel caso di compagnie statunitensi. Alcuni cittadini propongono la negoziazione di una convenzione internazionale per la protezione della privacy.

È importante sottolineare come la richiesta di leggi sul trattamento dei dati a fini commerciali attesti la mancanza di informazione sulla normativa esistente e sui provvedimenti del Garante per la protezione dei dati personali. Al contrario, i cittadini sono ben coscienti del sistematico trattamento dei dati da parte di compagnie con sede legale in un paese non appartenente all'Unione europea. La richiesta di una normativa europea uniforme va nello stesso senso del processo di adozione di un regolamento europeo sul trattamento dei dati personali attualmente in corso.

II. Informazione

- **Trasparenza istituzionale**

Tutte le raccomandazioni reclamano una maggiore trasparenza da parte delle istituzioni che trattano i dati ricavati dalle nuove tecnologie. Da un lato i cittadini chiedono che le autorità pubblichino i nomi degli

organismi, e anche dei responsabili, che trattano i dati a fini di sicurezza. Dall'altro chiedono che tali organismi rendano conto del loro operato attraverso la pubblicazione di resoconti delle loro attività.

- **Educazione e sensibilizzazione**

Un altro modo, molto sentito, di richiedere maggiore informazione è attraverso l'educazione e la sensibilizzazione dei cittadini rispetto al problema del trattamento dei dati personali a scopo di sicurezza raccolti tramite le nuove tecnologie. I cittadini propongono pubblicità progresso (comunicazioni sociali), campagne d'informazione su Internet, corsi nelle scuole per studenti ma anche corsi comunali per gli adulti.

III. Tutela istituzionale

Molti cittadini propongono la creazione di una nuova istituzione, un'autorità di controllo esperta e indipendente (nella maggior parte dei casi collocata a livello europeo, ma in alcuni casi anche a livello internazionale) che possa intervenire per sanzionare gli abusi degli organismi di sicurezza o dei governi. Inoltre, i cittadini ribadiscono che l'uso dei dati non dovrebbe avvenire senza l'autorizzazione di un'autorità giudiziaria.

Nessuna raccomandazione si rifà alle autorità esistenti, ad es. Garante Europeo, Gruppo di Lavoro dell'articolo 29, o i garanti di Europol ed Eurojust, autorità che hanno competenza a livello europeo in alcune delle aree menzionate dalle raccomandazioni.

IV. Tecnologia al servizio della privacy del cittadino

I cittadini chiedono un maggiore controllo sul funzionamento delle tecnologie, in particolare di poter controllare le funzioni che hanno un impatto sui propri dati personali. Domandano alle case produttrici, inoltre, di menzionare i rischi per la privacy nei manuali di funzionamento dei prodotti. Alcuni cittadini hanno proposto l'adozione di un "marchio" da apporre sui siti che rispettano il diritto alla riservatezza e alla protezione dei dati personali.

Senza nominarla, i cittadini sostengono la privacy by design, ossia il tener conto della privacy sin dalla fase di progettazione delle nuove tecnologie.

V. Alternative

Molti cittadini propongono l'impiego di alternative alle tecnologie per affrontare i problemi di sicurezza, sia nell'investigazione dei reati che nella gestione dei problemi di sicurezza delle comunità.

I partecipanti hanno anche potuto comunicare un messaggio specifico e inviduale attraverso le cartoline appositamente messe a disposizione (foto a sinistra). Questi messaggi faranno parte integrante del report finale.