IRISS
INCREASING RESILIENCE IN SURVEILLANCE SOCIETIES

Increasing Resilience in Surveillance Societies

Il diritto di accesso ai dati personali in Italia
Documento di sintesi e raccomandazioni

Dott.ssa Chiara Fonio e Dott.ssa Alessia Ceresa
Università Cattolica del Sacro Cuore, Milano
chiara.fonio@unicatt.it
alessia.ceresa@unicatt.it

Questo documento è una sintesi dei risultati di una parte della ricerca europea IRISS[1], dedicata all'esercizio dei diritti da parte dei cittadini. In particolare, la ricerca si proponeva di verificare l'effettiva capacità di accesso ai dati personali in ambiti pubblici e privati in dieci paesi europei. La trasparenza e l'accesso ai dati rappresentano, infatti, un aspetto cruciale dell'esercizio dei diritti democratici. In dettaglio, i cittadini sono legittimati a sapere chi è il titolare del trattamento, quali dati sono conservati e in che modo, se e con quali enti o soggetti terzi sono stati condivisi. Inoltre, essi hanno il diritto di verificare l'accuratezza di tali dati e di rivolgersi all'Autorità Garante in caso di reclami o segnalazioni.

Si premette che il "diritto di accesso" è garantito sia a livello comunitario sia nel contesto legislativo nazionale. In ambito europeo, infatti, l'argomento è disciplinato dalla Direttiva Europea 95/46/CE[2] "*relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati*". Essa prevede specificatamente alla Sezione V, intitolata "*Diritto di accesso ai dati da parte della persona interessata*", l'art. 12, in cui viene esplicato che cosa si intende per "diritto di accesso" in base al legislatore europeo. Ovvero, in particolare si garantisce che "*qualsiasi persona interessata ha il diritto di ottenere dal responsabile del trattamento*" tutti i propri dati personali; e che il "diritto di accesso" debba essere ottenuto "*liberamente e senza costrizione, ad intervalli ragionevoli e senza ritardi o spese eccessive (…)*"[3].

A livello nazionale, la legislazione si riferisce *tout cours* al Codice di protezione dei dati personali, D.Lgs. 30 giugno 2003 n. 196[4], il quale specificatamente e in attuazione della menzionata Direttiva Europea 95/46/CE, prevede espressamente il "diritto di accesso"

[1] http://irissproject.eu
[2] Parlamento Europeo e del Consiglio, Direttiva 95/46/CE del 24.10.1995, in G.U. delle Comunità europee, N° L 281/31-39, 23.11.95.
[3] Art 12, Parlamento Europeo e del Consiglio, Direttiva 95/46/CE del 24.10.1995, in G.U. delle Comunità europee, N° L 281/31-39, 23.11.95.
[4] D.L.gs. 30 giugno 2003 n. 196, in G.U. 29 luglio 2003 n. 174 – Supplemento Ordinario n. 123.

all'art.7 dello stesso Codice, completato da un assetto normativo volto a garantire l'esercizio[5] e la tutela[6] di questo medesimo diritto.

Nonostante il menzionato quadro normativo, i risultati della nostra ricerca mettono in luce molteplici criticità. Abbiamo, infatti, richiesto l'accesso ai nostri dati personali a 18 enti pubblici e privati[7]:

	Settore (pubblico o privato)	**Ente**
1	Pubblico	Videosorveglianza in ambito urbano
2	Pubblico	Videosorveglianza sui mezzi di trasporto
3	Pubblico	Videosorveglianza in un edificio governativo
4	Privato	Videosorveglianza in un negozio
5	Privato	Videosorveglianza in una banca
6	Pubblico	Uffici comunali
7	Pubblico	Motorizzazione civile
8	Pubblico	Europol
9	Privato	Videosorveglianza – Riconoscimento automatico targhe
10	Privato	Carta fedeltà – piccolo supermercato
11	Privato	Carta fedeltà – grosso supermercato
12	Privato	Compagnia di telefonia mobile
13	Privato	Banca
14	Privato	Carta di credito
15	Privato	Amazon
16	Privato	Twitter
17	Privato	Microsoft
18	Privato	Google

Nello specifico, abbiamo richiesto:

1. l'accesso a tutti i dati personali (art. 7, comma 1 e comma 2, lett. a) e b), Codice in materia dei dati personali)
2. quali dati personali sono stati condivisi e con quali enti e soggetti terzi (art. 7, comma 2, lett. e) Codice in materia dei dati personali)
3. la logica applicata ad un eventuale trattamento dei dati (automatico o non) (art. 7, comma 2, lett. c) Codice in materia dei dati personali)

Delle 16 risposte pervenuteci, **solo due, provenienti dal settore privato,** sono risultate complete e conformi alle nostre richieste.

Criticità:

- **I responsabili del trattamento**: in linea generale, i responsabili si sono mostrati sorpresi dalle nostre richieste, reiterando di "non aver mai ricevuto nulla di simile". Questo fa pensare che i diritti di accesso siano esercitati molto raramente da parte dei cittadini. Inoltre, abbiamo rilevato in pressoché tutti i casi una mancanza di

[5] Artt. 8 (*Esercizio dei diritti*), 9 (*Modalità di esercizio*) e 10 (*Riscontro all'interessato*) Codice di protezione dei dati personali

[6] Parte III-*Tutela dell'interessato*, Titolo I-*Tutela amministrativa e giudiziale*, Capo I-*Tutela dinanzi al Garante*, Sezione I-*Principi generali*, Art. 141 e ss. Codice di protezione dei dati personali

[7] Il documento completo con tutti i risultati della ricerca è consultabile a questo indirizzo: http://irissproject.eu/wp-content/uploads/2014/06/Italy-Composite-Reports-Final.pdf

conoscenza del quadro legislativo di riferimento. Aspetti soggettivi (la disponibilità del personale) prevalgono su aspetti oggettivi (preparazione giuridica e procedurale).

- **I sistemi di videosorveglianza**: è stato spesso difficile individuare i titolari del trattamento e solo in rari casi avevano un livello di preparazione adeguato, soprattutto in ambito pubblico. Questo ha comportato notevoli ritardi nel rispondere alle nostre richieste e continui solleciti da parte nostra. L'accesso alle immagini delle telecamere (garantito dall'art. 7, comma 1 del Codice in materia dei dati personali[8] e dal Provvedimento dell'Autorità Garante in materia di videosorveglianza 8 aprile 2010[9]) è risultato particolarmente problematico.

- **I diritti dei cittadini**: esercitare il diritto di accesso è visto "con sospetto", soprattutto nel settore pubblico nel quale i responsabili sono maggiormente abituati ad avere a che fare con richieste provenienti dalle forze dell'ordine che non dai cittadini. Inoltre, implica uno sforzo notevole da parte degli individui (non c'è quasi mai la possibilità di compilare un modulo online; occorre formulare la richiesta in modo giuridicamente corretto e sollecitare le risposte mancate o parziali).

- **Condivisione dei dati e trattamento automatizzato**: se è stato difficile ottenere l'accesso ai dati, ottenere informazioni circa l'eventuale condivisione con enti e soggetti terzi, nonché la logica del trattamento applicato, è stato praticamente impossibile.

- **Società multinazionali (es. Google, Twitter & co):** salvo rare eccezioni, in linea generale la prassi diffusa nel richiedere l'accesso ai dati è subordinata ad un'elevata conoscenza della lingua inglese**.**

- **Il ruolo del Garante della Privacy:** nonostante 5 segnalazioni (relative a cinque enti diversi) e 1 reclamo circostanziato presentato a Maggio 2014, per il quale sono stati pagati anticipatamente 150 euro di diritti di segreteria, non abbiamo riscontrato un effettivo e tempestivo interesse da parte dell'Autorità.

Raccomandazioni per l'implementazione di buone prassi

In base alle criticità riscontrate e all'esperienza maturata durante mesi di sopralluoghi e di corrispondenza con i titolari del trattamento, desideriamo esprimere le seguenti raccomandazioni:

1. I responsabili del trattamento dei dati devono essere individuati in modo chiaro e semplice, affinché gli individui interessati trovino velocemente tutte le informazioni necessarie. La possibilità di compilare una richiesta via web dovrebbe costituire la norma, non l'eccezione.

2. La formazione dei responsabili del trattamento e di eventuali membri dello staff deve essere adeguata ed aggiornata in base alla normativa nazionale e comunitaria.

---

[8] D.L.gs. 30 giugno 2003 n. 196, in G.U. 29 luglio 2003 n. 174 – Supplemento Ordinario n. 123.

[9] Garante per la protezione dei dati personali, *Provvedimento in materia di Videosorveglianza, 8 aprile 2010*: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680 (ultimo accesso 1 ottobre 2014).

3. I cittadini devono essere informati della possibilità di accedere ai dati personali che li riguardano e, soprattutto, non devono essere "guardati con sospetto" nel momento in cui esercitano un loro diritto.

4. Una volta stabilito il contatto con il responsabile del trattamento, le informazioni inerenti l'eventuale condivisione dei dati e il loro trattamento automatizzato o non, deve essere fornita al soggetto che la richiede in modo preciso.

5. Il responsabile del trattamento dovrebbe rispettare i 15 giorni indicati dall'Autorità Garante per fornire un idoneo riscontro.

6. Il reclamo all'Autorità Garante non dovrebbe essere garantito solo a "chi se lo può permettere". I costi del reclamo circostanziato sono eccessivamente elevati.

7. La comunicazione con l'Autorità Garante dovrebbe essere molto più snella ed efficace nelle sue conseguenze (es. intervento dell'Autorità).

8. Le informative sulla privacy e sul trattamento dei dati personali che si trovano sui siti web, si riferiscono nella maggior parte dei casi alla navigazione dei siti in oggetto (es. cookies), non a come esercitare il diritto di accesso. Le informazioni dovrebbero riguardare anche quest'ultimo aspetto.

9. Bisognerebbe rendere più chiaro se e in che modo i cittadini possono accedere alle immagini dei sistemi di videosorveglianza in ambito pubblico e privato.

10. L'informativa e la cartellonistica sulla videosorveglianza dovrebbero essere maggiormente omogenee e/o aderenti al fac-simile consigliato dall'Autorità Garante.