

Privacy vs Sicurezza, una falsa dicotomia?

Lucio Scudiero

Senior Fellow Istituto Italiano Privacy



ISTITUTO ITALIANO PER LA PRIVACY

Sicurezza e privacy. Verso un Safe harbour 2.0

IAIC

Roma, 9 Dicembre 2015



La tendenza in corso

«Io sono per aumentare i controlli, fare il riconoscimento facciale, mettere in comune le banche dati, far sì che tutte le telecamere siano a disposizione delle forze dell'ordine, io sono per taggare potenziali sospetti» Matteo Renzi, Digital Day, 21 novembre 2015



Il paradigma legale

*«la direttiva 2006/24 non prevede norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta. Pertanto, è giocoforza constatare che tale direttiva comporta **un'ingerenza nei suddetti diritti fondamentali di vasta portata e di particolare gravità nell'ordinamento giuridico dell'Unione**, senza che siffatta ingerenza sia regolamentata con precisione da disposizioni che permettano di garantire che essa sia effettivamente limitata a quanto strettamente necessario».*

C-293/12

SENTENZA DELLA CORTE - 8 aprile 2014

Un esempio: i PNRs

Nel recente accordo tra Consiglio e Parlamento su Direttiva PNR si prevede:

1. PNR= nome passeggero, date viaggio, itinerario, informazioni sul biglietto, dati di contatto, agente di viaggio presso cui il biglietto è stato acquistato, mezzi di pagamento usati, numero di posto e informazioni sul bagaglio
2. Finalità di prevenzione e repressione di minacce terroristiche o altri seri reati
3. Sia voli extra UE che intra UE
4. Conservazione= 6 mesi in chiaro e 4 anni e mezzo cifrati
5. Accesso da parte delle autorità identificate a livello di Stato Membro
6. Protocolli standard per lo scambio di dati tra Stati Membri
7. Possibilità di trattamento per controlli preventivi, quando criteri oggettivi di rischio lo impongano per identificare persone specifiche
8. Controllo delle autorità data protection degli Stati Membri

Criteri di proporzionalità fissati da CGE

«la normativa dell'Unione di cui trattasi deve prevedere **regole chiare e precise** che disciplinino la portata e l'applicazione della misura de qua e impongano **requisiti minimi** in modo che le persone i cui dati sono stati conservati dispongano di **garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi** nonché contro eventuali accessi e usi illeciti dei suddetti dati» §54

Criteri di proporzionalità fissati da CGE

«A questo proposito, si deve rilevare, in primo luogo, che la direttiva 2006/24 riguarda in maniera generale qualsiasi persona e qualsiasi mezzo di comunicazione elettronica nonché l'insieme dei dati relativi al traffico senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi» §57

Criteri di proporzionalità fissati da CGE

«Infatti, da un lato, la direttiva 2006/24 riguarda in maniera globale l'insieme delle persone che fanno uso dei mezzi di comunicazione elettronica, senza tuttavia che le persone i cui dati vengono conservati debbano trovarsi, anche indirettamente, in una situazione che possa dar luogo a indagini penali. Essa pertanto **si applica anche a persone per le quali non esiste alcun indizio tale da far credere che il loro comportamento possa avere un nesso, ancorché indiretto o lontano, con reati gravi.** (...)» §58

Criteri di proporzionalità fissati da CGE

«Dall'altro lato, pur mirando a contribuire alla lotta contro la criminalità grave, la suddetta direttiva non impone alcuna relazione tra i dati di cui prevede la conservazione e una minaccia per la sicurezza pubblica e, in particolare, non limita la conservazione dei dati a quelli relativi a un determinato periodo di tempo e/o a un'area geografica determinata e/o a una cerchia di persone determinate che possano essere coinvolte, in un modo o nell'altro, in un reato grave, né alle persone la conservazione dei cui dati, per altri motivi, potrebbe contribuire alla prevenzione, all'accertamento o al perseguimento di reati gravi» §59

Criteri di proporzionalità fissati da CGE

«In secondo luogo, alla suddetta mancanza generale di limiti si aggiunge il fatto che la direttiva 2006/24 non prevede alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore a fini di prevenzione, di accertamento o di indagini penali riguardanti reati che possano, con riguardo alla portata e alla gravità dell'ingerenza nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta, essere considerati sufficientemente gravi da giustificare siffatta ingerenza. Al contrario, la direttiva 2006/24 si limita a rinviare, all'articolo 1, paragrafo 1, in maniera generale ai reati gravi come definiti da ciascuno Stato membro nel proprio diritto interno» §60

Criteri di proporzionalità fissati da CGE

«Inoltre, per quanto riguarda l'accesso delle autorità nazionali competenti ai dati e al loro uso ulteriore, la direttiva 2006/24 non contiene le condizioni sostanziali e procedurali ad esso relative» §61

«In particolare, la direttiva 2006/24 non prevede alcun criterio oggettivo che permetta di limitare il numero di persone che dispongono dell'autorizzazione di accesso e di uso ulteriore dei dati conservati a quanto strettamente necessario alla luce dell'obiettivo perseguito. Soprattutto, l'accesso ai dati conservati da parte delle autorità nazionali competenti non è subordinato ad un previo controllo effettuato da un giudice o da un'entità amministrativa indipendente (...)» §62

Criteri di proporzionalità fissati da CGE

«Inoltre, per quanto riguarda l'accesso delle autorità nazionali competenti ai dati e al loro uso ulteriore, la direttiva 2006/24 non contiene le condizioni sostanziali e procedurali ad esso relative» §61

«In particolare, la direttiva 2006/24 non prevede alcun criterio oggettivo che permetta di limitare il numero di persone che dispongono dell'autorizzazione di accesso e di uso ulteriore dei dati conservati a quanto strettamente necessario alla luce dell'obiettivo perseguito. Soprattutto, l'accesso ai dati conservati da parte delle autorità nazionali competenti non è subordinato ad un previo controllo effettuato da un giudice o da un'entità amministrativa indipendente (...)» §62

Criteri di proporzionalità fissati da CGE

*«si deve aggiungere che tale direttiva non impone che i dati di cui trattasi siano conservati sul territorio dell'Unione, e di conseguenza non si può ritenere pienamente garantito il **controllo da parte di un'autorità indipendente**, esplicitamente richiesto dall'articolo 8, paragrafo 3, della Carta, del rispetto dei requisiti di protezione e di sicurezza, quali richiamati ai due punti precedenti. Orbene, **siffatto controllo, effettuato in base al diritto dell'Unione, costituisce un elemento essenziale del rispetto della tutela delle persone riguardo al trattamento dei dati personali** »*

§68

I criteri del Garante in materia di biometria

1. Previa Valutazione del rischio privacy;
2. Misure di sicurezza idonee;
3. deve essere privilegiata, laddove tecnicamente praticabile, la capacità di rilevamento della vivezza della caratteristica biometrica, basata sul rilevamento di differenti parametri di forma e fisiologici in modo da impedire grossolane falsificazioni della caratteristica biometrica impiegata.
4. Nella scelta dei processi biometrici si deve privilegiare l'uso di quelli che richiedono la cooperazione consapevole dell'interessato.
5. I dati biometrici grezzi (raw data) generati nel corso del procedimento di acquisizione biometrica (biometric capture) andranno cancellati da aree di memoria temporanea, centrale e secondaria e dal filesystem del sistema utilizzato per l'acquisizione immediatamente dopo la generazione del campione biometrico.
6. Il dato biometrico andrà possibilmente cifrato al momento della sua acquisizione dal sensore
7. La trasmissione del dato su canali di comunicazione cifrati;
8. Audit periodici sui sistemi;

Linee Guida Biometria <http://194.242.234.211/documents/10160/0/All+A+al+Prov.+513+del+12+novembre+2014+-+Linee-guida+biometria.pdf>

I criteri del Garante in materia di biometria

9. Conservazione dei campioni e modelli biometrici in aree di filesystem protette con strumenti crittografici o in database
10. che supportino la cifratura a livello di record o di colonna.
11. Evitare l'archiviazione centralizzata in banche dati accessibili su reti anche di tipo locale.
12. I dati identificativi degli utenti andranno conservati separatamente dai relativi dati biometrici.
13. Registrazione degli accessi ai dati biometrici, con log aventi caratteristiche di completezza, integrità, inalterabilità e durata della conservazione analoghe a quelle richieste per i log degli accessi di cui al provvedimento del Garante del 27 novembre 2008 sugli amministratori di sistema.
14. i campioni biometrici impiegati nella realizzazione del modello biometrico possono essere trattati solo durante le fasi di registrazione e di acquisizione necessarie al confronto biometrico, e non devono essere memorizzati se non per il tempo strettamente necessario alla generazione del modello stesso.
15. Venuta meno la necessità di trattare il dato questo deve essere cancellato in modo sicuro anche dalle aree di memoria volatile oltre che dai supporti di memorizzazione.

Linee Guida Biometria <http://194.242.234.211/documents/10160/0/All+A+al+Prov.+513+del+12+novembre+2014+-+Linee-guida+biometria.pdf>

Domanda conclusiva

La sorveglianza di massa è davvero efficace?



Giurista europeo specializzato in diritto ICT, privacy e protezione dei dati personali

Research Fellow e membro del Cda dell'Istituto Italiano Privacy, Lucio svolge attività di consulenza legale in Italia e in Europa per clienti multinazionali e start-ups innovative su un ampio spettro di questioni giuridiche legate al diritto delle nuove tecnologie. E' associato presso lo studio legle Ict Legal Consulting. Collabora al webmagazine Stradeonline, di cui è anche redattore.

LL.M in EU Law conseguito presso l'Università di Leiden (Olanda), Lucio ha acquisito esperienza anche in campo regolatorio lavorando presso lo European Data Protection Supervisor, a Bruxelles.

Autore di pubblicazioni scientifiche su giornali e riviste nazionali e internazionali, è anche fellow della European Privacy Association (EPA) e dell'Istituto Bruno Leoni.

www.istitutoitalianoprivacy.it

scudieroi@istitutoitalianoprivacy.it

Grazie dell'
attenzione!



ISTITUTO ITALIANO PER LA PRIVACY