CEPS Background Briefing

In preparazione per le Elezioni del Parlamento Europeo

Informando il Dibattito sulla Protezione dei Dati

Elspeth Guild, Sergio Carrera e Alejandro Eggenschwiler

Molti ambiti della politica europea saranno oggetto di un dibattito critico nella campagna elettorale in vista delle elezioni del Parlamento Europeo del 4-7 giugno 2009. Nonostante i temi specifici, e l'importanza che sarà loro attribuita, varieranno sostanzialmente da uno Stato membro all'altro, le materie riguardanti l'Area di Libertà, Sicurezza e Giustizia che sono diventate diritto e politiche dell'UE negli ultimi dieci anni meritano un'analisi informata e coerente. Esse, infatti, toccano nella sostanza il diritto di ogni individuo alla libertà e alla sicurezza in un'Europa allargata.

Questo Background Briefing verte sulla politica europea di protezione dei dati personali. Dopo aver delineato lo stato attuale della materia e gli sviluppi legislativi attesi nel prossimo futuro, il documento descrive i principali difetti e problematiche legati a questa politica. La sezione conclusiva evidenzia le sfide più importanti in quest'ambito e avanza delle raccomandazioni per i prossimi cinque anni.

Questo Background Briefing appartiene ad una serie di quattro documenti dedicati, rispettivamente, ai temi dell'immigrazione, dell'asilo, del controllo delle frontiere e della protezione dei dati personali, elaborati nell'ambito del progetto intitolato "Informando il Dibattito sull'Immigrazione in Preparazione per le Elezioni del Parlamento Europeo del 4-7 giugno 2009", finanziato dal Barrow Cadbury Trust, una fondazione indipendente dedita al finanziamento e alla promozione di iniziative per la giustizia sociale (per ulteriori informazioni, si visiti il sito http://www.bctrust.org.uk). L'obiettivo dei Background Briefings è quello di informare il dibattito su queste controverse, e spesso tecniche, tematiche per i partiti politici, mentre si preparano per le elezioni e si rivolgono agli elettori.

Elspeth Guild è Professore al Centro di Diritto dell'Immigrazione dell'Università Radboud di Nimega (Paesi Bassi) e Senior Research Fellow nella Sezione Giustizia e Affari Interni del CEPS. Sergio Carrera è Research Fellow e Capo della Sezione Giustizia e Affari Interni del CEPS. Alejandro Eggenschwiler è Assistente Ricercatore al CEPS.

Gli autori sono grati ad Alejandro Eggenschwiler per aver curato la traduzione all'italiano.

CENTRE FOR EUROPEAN POLICY STUDIES

Thinking ahead for Europe

BARROW CADBURY

1. Stato attuale della materia e sviluppi attesi

Il diritto alla protezione dei dati personali nell'UE si basa su un insieme di strumenti giuridici appartenenti sia al diritto internazionale che a quello europeo (per una lista completa delle misure adottate in materia di protezione dei dati, si veda l'Allegato). La "Direttiva sulla Protezione dei Dati"[1] del 1995 è lo strumento chiave in quest'ambito, in quanto stabilisce i principi generali che gli Stati membri devono seguire per garantire all'individuo il diritto alla riservatezza, assicurando, al contempo, la libera circolazione dei dati tra di loro. Essa disciplina le operazioni di raccolta, conservazione, elaborazione e diffusione dei dati personali tramite mezzi sia automatizzati (archivi elettronici) che tradizionali (archivi tradizionali), in relazione alle quali conferisce all'individuo un insieme di diritti quali il diritto ad essere informato circa il trattamento di dati che lo riguardano; il diritto ad ottenere la rettificazione, cancellazione o il blocco dei dati che non siano stati trattati in maniera conforme alla legge; e il diritto di ricorrere all'autorità giudiziaria in caso di violazione dei diritti di cui è titolare, durante il trattamento dei suoi dati. Per far fronte alle minacce poste dalle nuove tecnologie al diritto dell'individuo alla protezione dei dati personali, la Direttiva è stata affiancata da due ulteriori strumenti, riguardanti, rispettivamente, il diritto alla riservatezza nelle telecomunicazioni[2] e nelle comunicazioni elettroniche.[3] Il loro principale obiettivo è quello di garantire la confidenzialità nelle comunicazioni, proibendo l'ascolto, la registrazione e qualsiasi altra forma di intercettazione o sorveglianza non autorizzata.

Norme sulla riservatezza e sulla protezione dei dati personali sono contenute anche nella Convenzione europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali (art. 8), nella Convenzione 108[4] (entrambe adottate sotto gli auspici del Consiglio d'Europa) e nella Carta dei Diritti Fondamentali dell'UE (art. 7-8).[5] Occorre sottolineare, inoltre, che nell'UE esistono anche un Garante europeo della Protezione dei Dati[6] ed un Gruppo di Lavoro per la Tutela delle Persone con riguardo al Trattamento dei Dati Personali,[7] istituiti come organi indipendenti dotati di poteri consultivi e di supervisione. In particolare, il Garante assicura che le istituzioni e gli altri organi dell'UE trattino i dati personali in conformità alla norme pertinenti; formula pareri per gli organi decisionali dell'UE sulle nuove proposte legislative e su ogni questione suscettibile di incidere sul diritto degl'individui alla protezione dei dati; e coopera con le autorità nazionali per la protezione dei dati, al fine di ottenere un livello di protezione omogeneo in tutta Europa (per una lista dei pareri più recenti formulati dal Garante, si veda l'Allegato).[8] Il Gruppo di Lavoro, riunendo i rappresentanti delle autorità nazionali per la protezione dei dati, del Garante e della Commissione costituisce il foro di tale cooperazione.[9]

Tuttavia, mentre il quadro giuridico descritto sopra trova applicazione soltanto negli ambiti dell'ALSG raccolti nel Titolo IV del TCE (visti, asilo e immigrazione) – il cosiddetto "Primo Pilastro", questioni rilevanti ai fini della protezione dei dati possono sorgere anche nelle aree raccolte nel Titolo VI del TUE (cooperazione giudiziaria e di polizia in materia penale) – il cosiddetto "Terzo Pilastro", disciplinate dalla recente Decisione-quadro 2008/977/GAI sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale.[10] Questo divario è conseguenza del fatto che le politiche rilevanti per l'ALSG sono distribuite in due pilastri diversi e rischia di diminuire il livello e di minare la coerenza della protezione dei dati garantita nell'UE, specialmente alla luce del fatto che la citata decisione-quadro non è applicabile ad una serie di dati, tra cui: i dati raccolti per uso interno; i dati scambiati tra gli Stati membri e i paesi terzi in virtù di obblighi convenzionali e i dati trattati da Europol, Eurojust, dal Sistema d'Informazione Schengen (SIS) e dal Sistema Informativo Doganale (SID).

2. Difetti e problematiche legati alla politica europea di protezione dei dati

La costruzione dell'ALSG è stata guidata dalla ferma convinzione che la tecnologia sia la soluzione a tutti i problemi legati alla sicurezza, senza considerare che essa potrebbe produrre più insicurezza a causa delle tensioni che può generare con i diritti e le libertà dell'individuo, in particolare con il diritto alla protezione dei dati personali sancito all'Articolo 8 della Carta dei Diritti Fondamentali. L'UE ha sviluppato finora una serie di archivi elettronici e di sistemi per lo scambio di informazioni, tra cui:[11]

- EURODAC, una banca dati contenente le impronte digitali di tutti i richiedenti asilo e delle persone detenute per aver attraversato le frontiere dell'UE in maniera irregolare. Alla fine del 2007, EURODAC conteneva 1,086,246 insiemi di impronte, e nei primi cinque anni di funzionamento è costata 8.1 milioni di euro all'UE. In seguito ad un declino tra il 2005 ed il 2006, i dati mostrano un incremento del 19% tra il 2006 (165,958) ed il 2007 (197,284) nel numero di operazioni riguardanti i richiedenti asilo. In aggiunta, il numero di persone detenute per attraversamento irregolare delle frontiere è diminuito dell'8% nel 2007 (38,173).[12]
- Il Sistema di Informazione Schengen (SIS), una banca dati utilizzata dalle autorità degli Stati appartenenti all'Area

1 Direttiva 95/46/CE sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU 1995 L 281/31).

2 Direttiva 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni (GU 1998 L 24/1).

3 Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU 2002 L 201/37), modificata dalla Direttiva 2006/24/EC (GU 2006 L 105/54).

4 Convezione sulla Protezione delle Persone rispetto al Trattamento Automatizzato di Dati di Carattere Personale, Strasburgo, 1981.

5 GU 2000 C 364/1.

6 Art. 41 del Regolamento 45/2001/CE concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU 2001 L 8/1).

7 Art. 29 della Direttiva 95/46/CE.

8 http://www.edps.europa.eu/EDPSWEB

9 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

10 Decisione quadro 2008/977/GAI del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (GU 2008 L 350/60).

11 Per una panoramica completa sulle banche dati e i sistemi per lo scambio di informazioni dell'UE, si veda F. Geyer (2008), "Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom Security and Justice, CHALLENGE Research Paper n.9, May 2008, Centre for European Policy Studies, Brussels.

12 Commissione Europea, Relazione annuale al Consiglio e al Parlamento Europeo sull'attività dell'unità centrale EURODAC nel 2007, COM (2009) 13, Bruxelles, 26.1.2009.

Schengen per scambiare informazioni su determinate categorie di persone e di beni, che è stata utilizzata principalmente come archivio contenente i nominativi dei cittadini dei paesi terzi ai quali negare l'ingresso nel territorio dell'UE, e che si è evoluta nel SIS+ per includere anche i nuovi Stati membri del 2004. Quest'ultima, a sua volta, sarà trasformata, con accrescuite capacità, in un sistema di seconda generazione (SIS II).[13]

- Il Sistema di Informazione sui Visti (VIS), che conterrà informazioni su tutte le persone che richiedono visti per soggiorni di breve durata nell'UE.
- In aggiunta, la Commissione ha proposto la creazione di tre nuove banche dati di grande portata, nell'ambito del "Pacchetto Frontiere" del 2008, che sono: 1) un Sistema di Registrazione Ingressi/Uscite che registra i movimenti di determinate categorie di cittadini dei paesi terzi; 2) un Sistema Automatizzato di Controllo delle Frontiere capace di verificare automaticamente l'identità dei viaggiatori, siano essi cittadini UE o meno; 3) un Sistema Elettronico di Autorizzazione di Viaggio per ottenere informazioni personali dai viaggiatori che non sono cittadini dell'UE, tramite una verifica online prima della partenza (si veda il Briefing sul Controllo delle Frontiere).

Il contenuto e il modo in cui questi strumenti sono utilizzati danno origine ad un a serie di problemi.

In primo luogo, il "data mining" (estrazione di dati) è una delle questioni più delicate nel dibattito sulla protezione dei dati. I risultati delle ricerche condotte dalle autorità di polizia negli archivi possono presentare dei problemi, a seconda delle modalità di ricerca. Ad esempio, non essendo tutta la popolazione presente in tutte le banche dati, i sospetti tendono a ricadere solo sugli individui che presentano caratteristiche compatibili con quelle del profilo ricercato dalle autorità e che sono già presenti nella banca dati. Problemi diversi possono sorgere in relazione a ricerche di tipo diverso e, solitamente, si portano a termine una o più ricerche per individuo. Quelle condotte in base ad un profilo, che hanno luogo quando le autorità non sanno chi stanno cercando, pongono i problemi maggiori. Anche l'uso dei dati raccolti a scopo commerciale può creare dei problemi. Dunque, per evitare il rischio di danneggiare inutilmente l'individuo, i dati utilizzati dalle autorità di pubblica sicurezza devono essere accurati. I problemi sorgono quando i dati originali vengono integrati con informazioni più recenti, soprattutto nel momento in cui l'individuo è sotto l'attenzione delle autorità, ottenendo un profilo della persona del tutto arbitrario. Inoltre, i dati raccolti per motivi di pubblica sicurezza devono essere proporzionali ed adeguati allo scopo, in quanto la raccolta indiscriminata di dati non solo non è garanzia di maggiore sicurezza, ma costituisce anche una violazione del diritto dell'individuo alla riservatezza.

Un'altra questione importante è quella di assicurare che l'accesso ai dati sensibili sia strettamente limitato alle autorità cui spetta. L'accesso alle banche dati dell'UE dipende dallo strumento che le ha create. Ad esempio, l'accesso a EURODAC spetta soltanto alle autorità che devono verificare se un richiedente asilo lo ha già richiesto in un altro Stato membro (o è arrivato in maniera irregolare), ma sono stati compiuti dei passi verso la sua estensione a tutte le autorità di pubblica sicurezza. La natura dei soggetti legittimati ad accedere ad una banca dati, pertanto, e le conseguenze dell'estensione dell'accesso alle banche dati dell'UE anche alle autorità dei paesi terzi dovrebbero essere oggetto di un'attenta analisi al fine di garantire che i dati personali siano trattati in maniera adeguata e conforme alla legge.

Infine, gli individui devono essere adeguatamente protetti dalle conseguenze dell'inaccuratezza dei loro dati o dello scambio poco rigoroso degli stessi, e devono essere informati in maniera altrettanto adeguata dei diritti di cui godono in questi casi. Un sondaggio Eurobarometro del 2008 ha messo in evidenza che, mentre la maggioranza dei cittadini europei (64%) è preoccupata per la protezione dei propri dati, solo un quarto di loro (27%), circa, è a conoscenza dei diritti di cui gode in caso di un loro uso illegittimo, e neanche un terzo (29%) è consapevole del fatto che i dati sensibili, come quelli riguardanti la razza o le origini etniche, ricevono speciale protezione. Pertanto, i diritti dell'individuo in materia di protezione dei dati, e la sua informazione al riguardo, devono essere identificati come un altro argomento chiave del dibattito, al fine di eliminare le incoerenze che che attualmente minano il quadro giuridico europeo in quest'ambito, e soprattutto la sua applicazione all'ALSG. Il grado di protezione attualmente garantito a livello UE, infatti, è lungi dall'essere omogeneo, in quanto i diritti del soggetto dipendono ampiamente dalla banca dati in considerazione, e il divario tra gli standard raggiunti nei domini appartenenti rispettivamente al Primo e al Terzo Pilastro è ancora significativo.

3. Sfide future e raccomandazioni

Le seguenti questioni possono essere identificate come le principali sfide in relazione alla protezione dei dati personali nell'ALSG dell'UE:

In primo luogo, si dovrebbero inserire regole sulla riservatezza nei programmi operativi delle banche dati dell'UE, in modo tale da prevedere la cancellazione automatica dei dati dopo la scadenza del periodo consentito, prevenire l'accesso non autorizzato e la duplicazione di immagini sugli schermi dei computer e proibire le ricerche che non avvengono per ordine dell'autorità giudiziaria.

Inoltre, la creazione di banche dati dovrebbe essere preceduta da studi di valutazione d'impatto, realizzati da organizzazioni imparziali e indipendenti. Ogni strategia europea sullo scambio di dati deve iniziare con la valutazione e l'inventario delle politiche, degli strumenti e delle strutture istituzionali già esistenti nel campo della sicurezza a livello europeo. Le nuove banche dati dovrebbero essere create e utilizzate per finalità specifiche e compatibili con la legge, evitando definizioni generiche e raccolte di dati senza scopo.

Infine, i sistemi per la raccolta di dati non dovrebbero rivelare dati sensibili sulle origini etniche, le convinzioni religiose o altri aspetti vietati dalle norme anti-discriminatorie dell'UE. Pertanto, il ricorso a criteri nascosti indicanti distinzioni etniche o religiose, quali il luogo di nascita dei genitori o del soggetto stesso, o la loro precedente nazionalità, dovrebbe essere vietato.

13 Commissione Europea, Relazione sullo sviluppo del sistema d'informazione Schengen di seconda generazione (SIS II) - Relazione sullo stato dei lavori luglio 2008 – Dicembre 2008, COM (2009) 133, Bruxelles, 24.3.2009.

ALLEGATO

Misure adottate

1. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data (OJ 1995 L 281/31).
2. Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ 1998 L 24/1).
3. Regulation 45/2001/EC on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8/1).
4. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201/37).
5. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105/54).
6. Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ 2008 L 350/60).

Opinioni adottate dal Garante Europeo della Protezione dei Dati nel 2009

Supervisione

1. Opinion of 29 April 2009 on a notification for prior checking on Voice Logging at the Joint Research Centre Institute for Energy (JRC-IE) in Petten (Case 2008-014).
2. Avis du 1er avril 2009 sur la notification d'un contrôle préable à propos du dossier "Exercice annuel de retraite anticipée sans réduction des droits à pension" (Dossier 2008-719).
3. Avis du 30 mars 2009 sur la notification d'un contrôle préalable concernant le dossier "stagiaires structurels" (Dossier 2008-760).
4. Avis du 25 mars 2009 sur la notification d'un contrôle préalable à propos du dossier "traitement des demandes de levée de l'immunité de juridiction et d'inviolabilité des locaux et archives de la Commission" (Dossier 2008-645).
5. Avis du 23 mars 2009 sur la notification de contrôle préalable à propos de la gestion des informations transmises par l'OLAF dans le cadre du Memorandum of Understanding (Dossier 2009-011).
6. Avis du 10 mars 2009 sur la notification d'un contrôle préalable à propos du dossier Procédure de fin de stage (Dossier 2008-720).
7. Opinion of 26 February 2009 on a notification for prior checking regarding ETF - Flexitime procedure (Case 2008-697).
8. Avis du 23 février 2009 sur la notification d'un contrôle préalable à propos du dossier "Groupe de réintégration et de réorientation professionnelle" (Dossier 2008-746).
9. Opinion of 20 February 2009 on a notification for prior checking regarding the engagement and use of temporary agents (Case 2008-315).
10. Opinion of 18 February 2009 on a notification for prior checking on the procedure for early retirement without reduction of pension rights (Case 2008-748).
11. Opinion of 9 February 2009 on a notification for prior checking regarding "ART: Audit Reconciliation Tool" (Case 2008-239).
12. Avis du 26 janvier 2009 sur la notification de contrôlé préalable à propos du dossier "Menaces vis-à-vis des intérêts de la Commission dans les domaines contre intelligence, contre terrorisme" (Dossier 2008-440).
13. Opinion of 21 January 2009 on a notification for prior checking on the assessment of staff's capacity to work in a third language before first promotion (Case 2008-690).
14. Opinion of 21 January 2009 on a notification for prior checking concerning the report on probation period (Case 2008-604)
15. Opinion of 16 January 2009 on a notification for prior checking on the management of Central and Local Training SYSLOG Formation (Case 2008-481).
16. Avis du 16 janvier 2009 sur la notification d'un contrôle préalable à propos du dossier "Procédure relative aux commissions d'invalidité" (Dossier 2008-626).
17. Avis du 15 janvier 2009 sur la notification d'un contrôle préalable à propos du dossier "gestion et facturation de la crèche du Secrétariat Général du Conseil" (Dossier 2007-441).
18. Avis du 9 janvier 2009 sur la notification d'un contrôle préalable à propos du dossier "Exercice annuel de retraite anticipée sans réductions des droits à pension" (Dossier 2008-552).

Opinioni adottate dal Gruppo di Lavoro per la Tutela delle Persone con riguardo al Trattamento dei Dati Personali nel 2008

1. Opinion 3/2008 of the Article 29 Working Party on the World Anti-Doping Code draft International Standard for the Protection of Privacy.
2. Opinion 2/2007 on information to passengers about the transfer of PNR data to US authorities, Adopted on 15 February 2007 and revised and updated on 24 June 2008.
3. Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive).
4. Opinion 1/2008 on data protection issues related to search engines.