Dati sensibili, riservatezza e oblio

Il diritto alla protezione dei dati personali

Eventi rilevanti ed episodi di discriminazione e violenza

Novembre 2012 – Gennaio 2013 Cyberbullismo.
In soli tre mesi, la stampa ha dato notizia di due suicidi e un tentato suicidio di ragazzi vittime di denigrazioni in rete e da uno studio condotto dalla Società Italiana di Pediatria (SIP) risulta che il 34,2% degli adolescenti italiani ha fatto esperienza di cyber bullismo, direttamente o mediante propri amici.

Novembre 2012.
Un quindicenne di Roma si suicida, anche a seguito del dolore causatogli dalle continue denigrazioni di cui era vittima in ragione del suo orientamento sessuale, soprattutto attraverso la rete: gli era stato addirittura attribuito un profilo Facebook: "il ragazzo dai pantaloni rosa".

Gennaio 2013 Novara.
Una quattordicenne vittima di cyberbullismo si suicida, a quanto pare non tollerando più gli scherni subiti nei giorni precedenti, soprattutto sui social networks.

Gennaio 2013 Roma.
Un sedicenne, vittima di derisioni e bullismo, tenta il suicidio gettandosi dalla finestra dell'istituto scolastico da lui frequentato si suicida, a quanto pare

Gennaio 2013. Roma. Garante della Privacy sul diritto all'aggiornamento on-line delle informazioni.
Il Garante ordina a due gruppi editoriali . di predisporre, nell'ambito de loro archivio storico on line un sistema idoneo

a segnalare l'esistenza degli sviluppi delle notizie relative ad un ricorrente in modo da assicurare all'interessato il rispetto della propria (attuale) identità personale, quale risultato della completa visione di una serie di fatti che lo hanno visto protagonista e ad ogni lettore di ottenere un'informazione attendibile e completa (nel caso di specie dovrebbe darsi conto del completo proscioglimento dell'interessato da ogni addebito penale.

Ottobre 2013. Bergamo. Commercio di dati sanitari.
Alcuni giornali riportano la notizia di una sorta di "vendita", da parte di alcuni operatori sanitari, delle informazioni sullo stato di salute dei pazienti ricoverati al pronto soccorso di un ospedale. La gravità del caso è stata segnalata anche dal Garante, rilevando come sembri trattarsi di uno sfruttamento commerciale della conoscenza - per ragioni di ufficio - di dati personali altrui e, oltretutto, di dati meritevoli di una particolare protezione proprio perché idonei a rivelare lo stato di salute della persona e, quindi, anche a esporla a discriminazioni.

2013. Provvedimenti del Garante della Privacy contro Amministrazioni Comunali.
Nel corso del 2013 il Garante ha emesso provvedimenti inibitori nei confronti di circa 30 comuni, che hanno pubblicato in rete nominativi e patologie di soggetti sottoposti a trattamento sanitario obbligatorio, mal interpretando gli obblighi di pubblicità sanciti dalla normativa vigente. Analogo fraintendimento è alla base della pubblicazione in rete dei nominativi dei partecipanti a un concorso pubblico riservato a disabili, da parte di diversi istituti scolastici.

2013. Provvedimenti del Garante della Privacy contro soggetti pubblici e privati in relazione alla pubblicazione di dati biometrici.

Numerosi sono stati anche, nel corso dell'anno, i provvedimenti inibitori emessi nei confronti di vari soggetti, privati e pubblici (finanche istituti scolastici) per aver fatto ampio ricorso a sistemi biometrici di rilevazione delle presenze dei propri dipendenti, fondati quasi sempre sulla raccolta delle impronte digitali, in assenza dei presupposti legittimanti tale trattamento, che dev'essere residuale. In un caso, poi, la rilevazione delle impronte digitali per fini di controllo della presenza sul luogo di lavoro avrebbe potuto assumere un contenuto addirittura discriminatorio, essendo stata immaginata – nell'istanza formulata al Garante - come limitata ai soli dipendenti in esecuzione penale esterna.

2013. Provvedimenti del Garante della Privacy contro datori di lavoro in relazione alla videosorveglianza dei dipendenti.
Sono da segnalare - per quantità e importanza - i provvedimenti inibitori emanati dal Garante nei confronti di vari datori di lavoro, per aver sottoposto i lavoratori a videosorveglianza in assenza delle condizioni previste dallo Statuto dei lavoratori (accordo con le r.s.a. o autorizzazione dell'Ispettorato del lavoro). Si tratta di violazioni delle prime norme introdotte nell'ordinamento a tutela della riservatezza, in un contesto di tale sproporzione nei rapporti di forza - tra datore di lavoro e lavoratore -da rendere insufficiente il consenso del solo interessato (agevolmente condizionabile proprio per il potere contrattuale del titolare) da richiedere il coinvolgimento delle rappresentanze sindacali o, in assenza di un accordo in tal senso, di un organo istituzionale quale, appunto, l'Ispettorato del lavoro.

Quella del ricorso alla videosorveglianza anche in assenza di presupposti che la legittimino è tendenza frequente, a fronte di trattamenti carenti dell'informativa che anche in tali casi va resa all'interessato, sia pure in forma semplificata.

Particolarmente gravi sono poi i casi in cui le telecamere sono occultate al punto da non consentire in alcun modo all'interessato di rendersi conto di essere sottoposto a videoripresa.

22 Maggio 2013. Ravenna. Videosorveglianza in asili nido.
Il Garante ha vietato il ricorso a questa forma di videosorveglianza, realizzata - per stessa ammissione dell'istituto - per "tranquillizzare" i genitori più che per reali ragioni di sicurezza, con il rischio di ingenerare nel minore, fin dai primi anni di vita, la percezione che sia "normale" essere continuamente sorvegliati, come pure condizionare la spontaneità del rapporto con gli insegnanti.

24 maggio 2013 Roma. Telemarketing "selvaggio".
Il Garante della privacy ha emesso tre ordinanze ingiunzione per obbligare due importanti società di servizi informatici, specializzate nel settore delle banche dati , e un operatore Tlc al pagamento di sanzioni, pari a 800.000 euro, per aver violato provvedimenti prescrittivi già adottati nel loro confronti. Frequenti sono poi i casi di trattamenti illeciti di dati personali effettuati per fini di telemarketing, anche nei confronti di quanti si siano iscritti nell'apposito registro delle opposizioni.

Giugno 2013 Intercettazioni della National Security Agency.
Vengono rese pubbliche notizie in merito a una massiva e indiscriminata acquisizione di dati personali e di vere e proprie "intercettazioni" da parte della National Security Agency statunitense, a danno di cittadini non solo americani, con il ricorso alla disciplina speciale prevista dai Patriot Act (e in particolare dal Foreign Intelligence Surveillance Act), per fini di contrasto del terrorismo. Ineffetti, è probabile che dati di cittadini europei - quali interlocutori di statunitensi o comunque utenti di servizi, soprattutto di telecomunicazione, resi da aziende statunitensi - siano stati acquisiti dalle agenzie di intelligence americane, anche in virtù del double standard

che caratterizza la legislazione statunitense in materia, ammettendo per i non-citizens deroghe alle garanzie sancite invece per i cittadini rispetto all'azione investigativa. Anche di questa sorta di ultrattività della normativa americana nell'ordinamento europeo si è occupato un Tavolo di lavoro istituito dalla Vice-Presidente della Commissione europea Viviane Reding, nel quadro di una più generale revisione dei rapporti tra Usa ed Europa sul terreno delle reciproche garanzie del diritto alla protezione dei dati personali. I lavori del tavolo sono stati però fortemente ostacolati dall'opposizione, da parte degli Usa, del segreto finanche sull'interpretazione di concetti normativi fondamentali (es. "foreign intelligence") ai fini della conoscenza del reale impatto della disciplina dei Patriot Acts

Novembre 2013 . Strategia di azione per la tutela dei dati dei cittadini Europei.

La Commissione Europea elabora una strategia di azione (illustrata il 27 novembre 2013) comprensiva, in particolare, della conclusione, entro l'estate 2014, dei negoziati relativi all' "accordo-ombrello" tra Europa e Usa per la tutela dei dati personali nel settore della cooperazione di polizia e giudiziaria, unitamente al rafforzamento dell'Accordo di mutua assistenza giudiziaria Ue-Usa del 2010 (e di quelli, correlati, di settore), così da garantire rimedi giurisdizionali ai cittadini europei; la previsione tassativa dei casi nei quali le autorità europee possano cedere dati agli organi americani e dei termini di conservazione dei dati stessi, nonché delle condizioni per la loro utilizzazione. In ogni caso, i trasferimenti di dati dalle autorità europee a quelle americane potrebbero avvenire solo nei casi espressamente previsti da appositi accordi bilaterali. Si tratterebbe, nel complesso, di previsioni importantissime, in quanto relative ai punti di maggiore criticità della disciplina americana. La strategia della Commissione prevede anche la revisione, entro l'estate 2014, degli accordi Safe Harbour che regolano la cessione di dati alle aziende Usa, tale da garantire

ai cittadini europei adeguate possibilità di ricorso mediante Adr (modalità stragiudiziali di risoluzione delle controversie) in caso di violazioni della privacy; maggiore trasparenza nelle privacy policies delle aziende, così da rendere l'utente (anche straniero) edotto dei rischi cui possa essere esposto; maggiori controlli, da parte del Governo Usa, sul rispetto dell'accordo da parte delle aziende con coinvolgimento delle Autorità di protezione dati di volta in volta competenti in caso di sospetta inottemperanza.

Novembre 2013. Italia Misure per la difesa da minacce cibernetiche.
Importantissima – e senza precedenti in Europa – la sottoscrizione, l'11.11.2013 di un protocollo d'intenti con il Dipartimento per l'informazione e la sicurezza dello Stato, (che consente tra l'altro, l'accesso alle banche dati dei fornitori di servizi di comunicazione da parte dei Servizi) e all'estensione dei poteri delle Agenzie d'intelligence al campo della cybersecurity. Il protocollo disciplina alcune procedure informative specifiche e innovative, perché di carattere sistematico e inerenti le modalità di svolgimento dei trattamenti per fini d'intelligence, nel rispetto delle cautele previste dal Codice. Tale forma di esercizio dei poteri di garanzia dell'Autorità è, infatti, maggiormente corrispondente alle peculiarità che caratterizzano oggi le attività delle Agenzie d'intelligence e i loro poteri di "accesso sistematico" come ampliati dalla l. 133/2012, in conformità, peraltro, a una tendenza globale connessa ai crescenti rischi derivanti da minacce cibernetiche.

Raccomandazioni

1. Inserire , nel novero dei soggetti titolari del diritto alla protezione dati gli enti e le associazioni. Tale riforma potrebbe poi essere bilanciata da una generale revisione e un aggiornamento degli adempimenti previsti dal Codice a carico dei titolari del trattamento.

2. Rivedere il sistema sanzionatorio previsto dal Codice per gli illeciti amministrativi e quelli penali, con una complessiva riforma che abbia come linee guida: l'esclusione di deroghe al principio di assorbimento dell'illecito penale in quello amministrativo; la previsione della procedibilità a querela per il delitto di trattamento illecito di dati personali; la depenalizzazione di molti reati d'inosservanza privi di reale offensività verso terzi; l'introduzione di ulteriori clausole di non punibilità (sia per illeciti amministrativi, sia per illeciti penali) in presenza di condotte riparatorie e forme di ravvedimento operoso da parte dell'autore.

3. Escludere espressamente dagli obblighi di pubblicità di dati personali, sanciti per fini di trasparenza dell'azione amministrativa, i dati da cui possano evincersi informazioni relative allo stato di salute o alla condizione economico-sociale di particolare fragilità dell'interessato.

4. Introdurre una disciplina ad hoc del trattamento dei dati biometrici che non legittimi l'ampio ricorso che oggi comunemente se ne fa, in particolare prevedendo i presupposti necessari per garantire la reale spontaneità del consenso da parte degli interessati.

5. Attuare l'art. 53 del Codice, nella parte in cui rimette a un decreto del Ministro dell'interno il "censimento" delle banche dati istituite per fini di pubblica sicurezza, così da consentire agli interessati la tutela dei propri dati personali, anche per i trattamenti svolti a fini di giustizia. Inoltre vanno normate in maniera stringente le modalità di applicazione del Codice alle attività di intelligence.

6. Intervenire sul piano legislativo al fine di limitare le possibilità di utilizzazione da parte delle forze di polizia di dati personali (soprattutto se sensibili, giudiziari o genetici) a quelli effettivamente indispensabili per il perseguimento degli obbiettivi di prevenzione e accertamento dei reati e per i quali si possa effettivamente svolgere un'efficace attività di difesa.

7. Prevedere nel regolamento di attuazione della istituenda banca-dati del DNA che i tempi di conservazione dei profili genetici siano commisurati alla rilevanza delle informazioni genetiche per le specifiche esigenze di accertamento di ciascun tipo di reato.

8. Introdurre, come auspicato dalla stessa giurisprudenza costituzionale e di legittimità, una specifica disciplina dell'utilizzazione processuale delle videoriprese realizzate in luoghi di privata dimora, estendendo espressamente a quelle che abbiano natura "captativa" di conversazioni il regime previsto per le intercettazioni tra presenti.

9. In particolare sarebbe auspicabile: 1) codificare e limitare l'utilizzo delle registrazioni di conversazioni fra presenti realizzate ad insaputa degli interessati, ad oggi ritenuta legittima; 2) aggiornare il Codice deontologico dei giornalisti, anche stabilendo garanzie ulteriori per i soggetti meritevoli di una tutela rafforzata – quali i minori e le vittime – e per l'effettivo rispetto della presunzione d'innocenza,

3) definire specifiche misure a garanzia del diritto all'oblio dell'interessato.

10. Assicurare l'effettività del diritto alla protezione dei dati personali nei luoghi di privazione della libertà, promuovendo la consapevolezza del diritto in parola tra detenuti, internati, stranieri trattenuti nei Cie.