ISTITUTO ITALIANO PRIVACY

PER UNA PRIVACY PIU' PUBBLICA, PIU' LIBERA, MENO BUROCRATICA

I SUGGERIMENTI DELL'ISTITUTO ITALIANO PER LA PRIVACY AL NUOVO COLLEGIO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

25 giugno 2012

Cogliendo l'occasione di un articolato "temario-questionario" sottoposto pubblicamente da Agorà Digitale a tutti i candidati al Collegio del Garante, prima dell'elezione da parte del Parlamento, l'Istituto intende fornire alcuni punti di vista tecnici e di *policy*, sperando si rivelino preziosi per il programma dell'Autorità nel prossimo, importantissimo settennato.

---

1. Impatti della normativa privacy per la pubblicità on line, appena approvata dal Governo in recepimento della Direttiva Cookie emanata dall'Unione Europea

Questa nuova normativa, introdotta dal Decreto legislativo 69/2012 in recepimento della Direttiva 2009/136/CE, comporta l'obbligo del consenso preventivo dell'utente prima di poter usare cookies che lo profilano per fini ulteriori, tra cui quello di marketing. Fermo restando il diritto del navigatore di scegliere se ricevere o meno cookies, per poter valutare adeguatamente gli impatti di questa norma occorre evitare le astrazioni. Tutto, in effetti, si gioca nella scelta delle modalità semplificate per sottoporre all'utente l'informativa e ottenerne il consenso, su internet. Sarà il Garante a dover stabilire, con un suo provvedimento, queste modalità: dovrà farlo tenendo conto del parere delle associazioni di categoria interessate (consumatori, operatori di internet e del marketing). E' cruciale individuare metodi facili, al passo coi tempi, che non appesantiscano l'esperienza di navigazione dell'utente e, al contempo, non "ammazzino" il mercato pubblicitario on line. Anche in questo caso ci vuole equilibrio: se da un lato occorre dare potere all'utente di decidere in merito ai cookies, dall'altro occorre non dimenticarsi che non esiste il "diritto fondamentale a Google" e che molti servizi gratuiti su internet vivono grazie alla pubblicità personalizzata. Per cui anche i cookies utilizzati a fini di profilazione commerciale vanno adeguatamente disciplinati ma non resi impossibili da utilizzare.
Vedremo come verrà attuato in pratica il riferimento – contenuto sia nella direttiva 2009/136 sia nel dlgs n. 69/2012 di suo recepimento - della possibilità di esprimere il consenso ai cookies tramite la configurazione del software di navigazione o browser. Anche su questo aspetto si gioca la partita dell'efficacia della norma.

2. Quali Provvedimenti Generali e in quali settori si ritengono essere i più urgenti da adottare, da parte del Garante Privacy, per assicurare il rispetto e l'implementazione dei principi fondamentali della privacy che vigono in Italia

Il potere nomofilattico spetta al Parlamento ma il Garante, nell'ambito delle proprie competenze, ha interessanti prerogative che andrebbero meglio utilizzate al fine di

consentire un ottimale adeguamento della vigente disciplina a tutela dei dati personali alle esigenze del mercato e per la efficace protezione degli individui. Il riferimento va all'istituto del bilanciamento di interessi ed all'iter per la creazione dei codici deontologici da allegare al codice privacy. Attraverso il bilanciamento d'interessi in determinate circostanze, anche di carattere generale, il Garante può esonerare il Titolare dall'ottenere il consenso degli interessati quando ritiene che l'interesse perseguito da quest'ultimo sia legittimo e, anche grazie a misure alternative di tutela, non prevalgano i diritti dei soggetti a cui si riferiscono i dati. Un ragionato ricorso a questo istituto potrebbe consentire di intervenire in alcuni settori e situazioni in cui l'attuale disciplina è avvertita come eccessivamente rigorosa senza apportare, di converso, effettivi benefici alle aspettative di tutela dei cittadini. Finora, il Garante si è avvalso di questo istituto in misura esigua.

Il secondo punto riguarda la creazione di codici deontologici previsti in via generale dall'art. 12 del codice privacy. Il Garante ha il potere di promuoverne la sottoscrizione per determinati settori; in questo modo si può far ricorso ad una fonte normativa alternativa alle leggi, formata in via autodisciplinare dalle medesime categorie interessate, maggiormente competenti a disciplinare le proprie attività, le quali partecipano alla sua formazione nel rispetto del principio di rappresentatività. Si tratta di una pregevole innovazione del codice privacy che fornisce alla disciplina autodiretta, lungimirante esempio di democrazia orizzontale o "dal basso", valenza di forza di legge con efficacia generale e non solo circoscritta all'interno della categoria di riferimento. Anche questo potere di promozione andrebbe utilizzato più diffusamente. Peraltro, il coinvolgimento delle imprese dei settori coinvolti ha il merito che le regole contenute nei codici deontologici siano tecnicamente aderenti alle realtà operative, talvolta complesse, e siano meglio recepite dal mondo imprenditoriale che ne è il destinatario.
Un esempio calzante in questo ambito sarebbe la disciplina da applicare al cloud computing (di fatto, la nuova realtà delle forniture di "servizi" di tecnologia hardware e software in outsourcing) tanto tecnica e complessa da giustificare il ricorso allo strumento del codice deontologico: il Garante ha rilasciato in questi mesi due documenti (Schede di documentazione e, da poco, un opuscolo informativo), che non hanno valore normativo vincolante. Ciò che il mercato chiede, invece, sono regole chiare e puntuali: ormai le forniture cloud sono diffuse sia nel settore privato sia nel pubblico, e dobbiamo garantire norme certe agli operatori. Naturalmente, nonostante le indubbie difficoltà di regolazione, siamo certi che questa soluzione potrebbe portare la normativa avanti, pur senza strappi con l'attuale Codice privacy. Ed un maggiore ricorso ai codici deontologici offrirebbe anche un migliore posizionamento di ruolo alle linee guida, che hanno svolto un compito positivo e sono state un fiore all'occhiello del Garante in questi anni: esse – previa consultazione pubblica in fase di emissione e di aggiornamento periodico – potrebbero corroborare i codici deontologici per settore, con ricchezza di esempi specifici e concreti.

Un terzo aspetto che meriterebbe attenzione è il Piano semestrale delle ispezioni: sarebbe opportuno documentare e motivare le ragioni in base alle quali il Garante decide di effettuare ispezioni in un determinato settore, nei successivi sei mesi. E' bene che l'Autorità espliciti con trasparenza, quali sono le giustificazioni di una determinata attività ispettiva generale "per categoria o settore". Questo aiuterebbe i Titolari del trattamento di quello

specifico settore a capire in tempo le criticità privacy più rilevanti e ad adeguarsi meglio. Dopotutto, sarebbe utile come opera di diffusione di consapevolezza e di compliance. Un approccio ragionevole e persuasivo, insomma.

Ulteriore profilo è una maggiore attenzione del Garante al settore pubblico, che storicamente è stato oggetto di meno verifiche che hanno portato a sanzioni (mentre possiamo immaginare che anche parecchi uffici pubblici abbiano rilevanti questioni privacy da risolvere con urgenza).

Infine, avrebbe senso un Provvedimento dedicato ai dati dei bambini, minori di 13 anni: nel nostro Codice privacy sono poche le disposizioni a tutela dei bimbi, mentre servirebbero indirizzi generali su come rispettarne al meglio la riservatezza e l'identità. Questo dovrebbe avvenire parallelamente ad un forte lavoro nelle scuole: finora il Garante ci ha provato, saltuariamente e simbolicamente, distribuendo materiale divulgativo per gli studenti e facendo qualche evento nelle scuole. Splendide attività. Ma il Garante che vorremmo guarderebbe e parlerebbe agli insegnanti, oltre che agli studenti, perché sono loro ad accompagnare giorno dopo giorno i ragazzi, quindi immaginiamo una strettissima collaborazione tra Garante e Ministero dell'Istruzione, dell'Università e della Ricerca.

Nell'ipotizzare un Provvedimento generale, affronteremmo anche il grande tema degli "User Generated Contents", cioè di tutti quei trattamenti di dati per finalità esclusivamente personali che tuttavia comportano diffusione o comunicazione sistematica grazie alle nuove tecnologie (ognuno di noi ha smartphone e condivide sul web miriadi di contenuti, anche altrui): non imponendo censure o divieti, ma reinventando tutto l'insieme di avvisi di rischio e di informative privacy, in modo che si radichi piena padronanza nell'uso di questi sistemi da parte degli utenti, limitando fortemente la probabilità di violazioni "orizzontali", diffuse.

3. I temi e le questioni più stringenti da portare in Europa, intorno al tavolo del WP29 (Gruppo di lavoro dei Garanti Privacy europei)

Senza dubbio la privacy su Internet, la necessità di insistere per un Internet Bill of Rights condiviso a livello europeo e, quindi, globale e la ricerca di nuove reciprocità tra UE e Paesi extra-UE. Poi, ovviamente, si dovrebbe spingere sull'acceleratore per intervenire autorevolmente nel dibattito che si sta svolgendo intorno alla discussione parlamentare europea, oggi in corso, sulla nuova Proposta di Regolamento privacy. Su quel terreno ci giocheremo i prossimi vent'anni di data protection per cittadini, istituzioni e imprese europee.

4. Riflessioni su Serpico, il sistema pubblico di monitoraggio delle spese e dei conti bancari per contrastare l'evasione fiscale

La norma che istituisce questo tipo di controllo massivo è stata dettata dall'emergenza: l'evasione fiscale in Italia è drammatica e bisogna scovare una moltitudine di soggetti silenziosi per riportare equità nel sistema fiscale (fermo restando che siamo convinti non abbia molto senso "chiedere" trasparenza sulle vite private senza parallelamente "dare" la massima trasparenza su spese e procedimenti selettivi pubblici). Ciò detto, in quella legge c'è un difetto duplice: 1. si controllano tutti, per trovare qualcuno; 2. non c'è una data di

scadenza. Il controllo generalizzato (sproporzionato) a priori di decine di milioni di presunti innocenti ha il sapore amaro dello Stato di polizia, in cui la sicurezza e la legalità sono massime ma si perde la libertà. L'operazione riesce perfettamente, e il paziente muore. Proprio per questo, una norma così eccezionale avrebbe dovuto nascere con la "*expiration date*" già assegnata. Se fossimo nel Garante, proporremmo subito una segnalazione alla Commissione Europea, perché valuti se avviare una procedura per possibile contrasto con i Trattati e la Carta dei Diritti Fondamentali della UE.

5. Il Codice Privacy, in alcune parti, è rimasto inattuato: ecco quali sono i punti più rilevanti di competenza del Garante, ai quali porre subito mano attuativa

In primo luogo, come già detto, rivolgeremmo forti attenzioni agli articoli del Codice privacy che riguardano il settore della pubblica amministrazione: è fondamentale intervenire affinché quelle regole vengano pienamente rispettate in ogni ufficio pubblico. Uno Stato non "compliant" fa fatica ad esigere adempimenti dagli operatori privati. I dati di milioni di cittadini devono essere protetti al massimo livello.

Diverse norme del Codice privacy prevedono, poi, che il Garante debba promuovere l'adozione di Codici deontologici privacy di settore (tipo quello per l'attività giornalistica), ma sono inattuate. Pensiamo al Codice deontologico sul Marketing diretto (art. 140), a quello su Internet (art. 133), a quello sulle Informazioni Commerciali (art. 118, che in sostanza significa un Codice sui dati e comportamenti dei debitori, perché queste sono le "informazioni commerciali", e la cosa appare particolarmente significativa in tempi di crisi economica e di difficoltà umane ad essa connesse). Apriamo più tavoli, fidiamoci della società civile, approviamo questi codici.

6. In che modo potrebbe il Garante svolgere il suo compito tutelando i diritti dei cittadini relativi alla sfera della privacy senza ostacolare le esigenze di mercato?

Una prima osservazione di base riguarda l'auspicio che il rapporto tra l'istituzione del Garante ed il mondo imprenditoriale sia riposizionato su una piattaforma di leale confronto e reciproca fiducia, sebbene nella distinzione dei ruoli. Devono crollare i muri della reciproca diffidenza che tanto nuocciono alle istituzioni, alle imprese ed al Paese in genere. Occorre una maggiore trasparenza e condivisione ed i citati suggerimenti verso un migliore utilizzo dell'istituto del bilanciamento di interessi e verso il ricorso ai codici deontologici, vanno proprio in questa direzione.

In secondo luogo, occorre tener presente che il nuovo regime legale promosso dalla proposta di Regolamento UE si basa sull'imposizione di un modello aziendale di gestione e controllo a tutela dei dati personali. La corretta compliance aziendale nell'agire quotidiano consentirà la tutela dei diritti dei cittadini senza sovrastrutture burocratiche imposte da onerosi adempimenti. La Commissione europea, prima, ed il Garante nazionale, dopo, svolgono un ruolo fondamentale affinchè questo progetto si attui nel migliore bilanciamento.

Tramite il cambio di approccio culturale di cui si accennava nonché, attraverso l'introduzione e ufficializzazione delle metodologie e delle prassi amministrative ispirate ad esperienze di altri Paesi (anche europei), il Garante potrebbe assumere il ruolo di "tutor" per le imprese, accompagnandole nel percorso di compliance senza adottare da subito

ingiunzioni o applicare sanzioni. Ci piacerebbe immaginare che un Membro del Collegio, a turno, facesse da "sportello" verso il pubblico almeno una volta alla settimana.

7. Copyright: prevale il diritto alla privacy ?
Il copyright, magari ammodernato, va protetto. I delinquenti che traggono profitti dalla pirateria vanno perseguiti. Chi, tuttavia, pensasse che la soluzione sia applicare filtri alla Rete o un setaccio massivo a priori alle comunicazioni on line di milioni di utenti, per il solo fatto di combattere la pirateria informatica, si sbaglierebbe di grosso. Tutto ciò che consiste in intercettazione (chiamiamo le cose con il loro nome) senza ordine di un magistrato può ledere i diritti costituzionali dei cittadini-utenti. Anche in questo caso si tratta di un equo bilanciamento tra valori apparentemente contrapposti e la giurisprudenza consolidata della Corte di Giustizia ha già precisato che, in caso di conflitto, l'arretramento della tutela dei dati personali, oltre a dimostrarsi essenziale, per consentire l'esercizio del valore contrapposto non può spingersi sino al punto di trasformarsi in un sostanziale azzeramento di tale diritto fondamentale.

8. Che ruolo può avere il Garante privacy per agevolare il Riuso di dati pubblici da parte dei soggetti interessati al loro utilizzo e favorire quindi il principio della trasparenza dei dati delle pubbliche amministrazioni?
La privacy non rappresenta già oggi, in moltissimi casi, un ostacolo né al riuso dei dati pubblici né alla trasparenza amministrativa. Il problema è l'ignoranza delle facoltà di riuso, spesso, insieme al timore di fare "passi falsi". Il Garante potrebbe fare una cosa semplicissima e, al contempo, dirompente in senso buono: chiarire con un Provvedimento (a cui allegare un vademecum) come le Pubbliche Amministrazioni possano agevolmente riutilizzare i dati personali (per esempio spiegando loro come anonimizzarli per destinarli al riuso). Acqua calda, ma finché non apriamo il rubinetto tutto resterà (quasi) fermo. Poi, crediamo si debba rivedere la disciplina in materia di accesso ai documenti amministrativi e di segreto d'ufficio, ma ciò esula dalle competenze del Garante.

9. Va aggiornato il Codice deontologico privacy per il giornalismo?
Del valore dei codici deontologici abbiamo già detto e quello per il giornalismo ha un valore particolare: regolamentare la libertà di informazione ed il diritto di cronaca, evitando abusi, è impresa non facile. Il fatto di esserci riusciti con generale soddisfazione tramite la sottoscrizione del codice deontologico e la Carta di Treviso andrebbe valorizzato molto più di quanto sia stato fatto. In primo luogo occorrerebbe che il codice deontologico – che è norma di legge – fosse fatto rispettare.

L'eventuale aggiornamento dovrebbe vedere la partecipazione di soggetti ulteriori e diversi rispetto a quelli che furono coinvolti allora, alla fine degli anni '90: non solo giornalisti, dunque, ma anche, ad esempio, categorie di nuovi attori dell'informazione, consumatori, associazioni di provider, associazioni di parenti di vittime di reati. Inoltre, sarebbe opportuno che un futuro codice 2.0, si avvalesse di linee guida contenenti indicazioni concrete (tipo FAQs, per esempio spiegando quando informazioni su salute e vita sessuale non sono essenziali con casistiche specifiche), e non solo principi generali che rinviino a futuri eventuali pronunce puntuali, come già suggerito in precedenza (peraltro, in questo

senso, potrebbe utilizzarsi operativamente il lavoro editoriale già svolto dal componente del precedente Collegio, Mauro Paissan). Tra i nuovi nodi da sciogliere vi è quello della privacy dei defunti sui media, finora mai affrontato, e l'obbligo di aggiornamento delle notizie comparse in testate on line, tema affrontato in senso positivo in una sentenza della Cassazione che ha fatto scalpore e che suggerirebbe una disciplina articolata. Infine è arrivato il momento di ragionare sul fatto che l'informazione è ormai tecnologica, quindi il Codice dovrebbe focalizzarsi anche sul (e differenziare in base al) modo di utilizzo delle tecnologie, nel dettaglio, poiché il singolo strumento-mezzo può generare impatti/messaggi diversi.

10. Quali misure sono necessarie per rendere effettivamente equilibrato il rapporto tra privacy dell'interessato, diritto all'oblio e diritto di cronaca e di critica?

Anche questo è un esempio di confluenza di valori diversi, apparentemente confliggenti. Come già evidenziato in precedenza, occorre trovare l'equo bilanciamento che tenga conto della libertà di informare e di essere informati, del diritto di espressione del proprio pensiero, insieme ai diritti di pertinenza, correttezza ed essenzialità delle informazioni. Tra questi vi è il diritto a ritirare dalla circolazione quei dati personali che abbiano esaurito la propria funzione informativa, in base alla finalità d'uso originaria. Il problema ha carattere generale ma è esploso con Internet che è la piattaforma informativa che tutto contiene, diluendo fortemente il potere di controllo dell'individuo sull'uso dei dati personali che lo riguardano. Una notizia ancorché vera e correttamente pubblicata in rete, può risultare in contrasto con legittimi interessi del data subject se rimane disponibile per un tempo indefinito, trasformandosi in un dato storico. Prima dell'avvento di internet, l'informazione "datata" avrebbe riguardato solo figure di rilevanza storica, mentre oggi essa può interessare un cittadino qualunque. La persistenza dell'informazione, sganciata dal profilo di interesse storico del personaggio, può condizionare il libero sviluppo della personalità individuale, cristallizzando fatti, opinioni, notizie con un appiattimento informativo, scollegato dall'elemento temporale, che può ledere la dimensione di libertà umana: la libertà di cambiare opinione e di essere diversi nel corso degli anni. Di conseguenza, se misure automatizzate per garantire l'aggiornamento di tutte le notizie presenti on line, come raccomandate in una recente e importante pronuncia della Cassazione, possono sembrare eccessivamente onerose e di difficile realizzazione, il principio della conservazione dei dati limitata nel tempo va preservato. Il principio dell'aggiornamento non è assoluto; il codice privacy, infatti, lo prescrive come obbligatorio solo "se necessario" e il caso oggetto della sentenza della Cassazione citata ne è un esempio palese: i giudici di legittimità hanno ritenuto che l'editore on line fosse tenuto all'aggiornamento in quanto la notizia rintracciabile con i motori di ricerca riguardava l'incarcerazione di un politico a seguito di un'accusa per corruzione (eravamo all'apice di tangentopoli), successivamente caduta nel vuoto per insussistenza dei fatti. Anche in base al comune senso di giustizia si sarebbe potuto ritenere che il politico coinvolto abbia diritto a far sì che, insieme alla notizia del suo arresto, vi fosse anche quella del suo totale proscioglimento. Il caso riportato, più di altre considerazioni, attesta come l'equo bilanciamento vada perseguito valutando i fatti specifici ed evitando il difetto di astratte generalizzazioni.

11. "Web libero", privacy e sicurezza: equilibrio e proporzionalità

Uno Stato democratico fonda la propria forza nella ricerca di un equo bilanciamento tra valori diversi. Pertanto, come già scritto a proposito dei controlli massivi fiscali e dei filtri alla Rete per tutela del copyright, ci opporremmo pubblicamente a qualsiasi tentativo di spostare tale equilibrio su un asse di prevaricazione sproporzionata ed eccedente di taluni interessi a danno di altri diritti fondamentali: così tra sicurezza pubblica e tutela dei dati personali e viceversa, tra repressione degli abusi al SSN e tutela della dignità del paziente, fra libertà di informazione e dignità dei singoli. Ma gli esempi potrebbero essere molti ancora e rilevanti.

12. La promozione della cultura della Privacy presso i fornitori di servizi di comunicazione elettronica, i servizi a valore aggiunto e i fornitori di applicazioni

Come già chiarito a proposito del bilanciamento tra libertà economiche e diritti fondamentali, crediamo fortemente nell'auspicabile ruolo di persuasione attiva svolto dal Garante, che può trasformarsi in un "tutor" per consentire ai fornitori di servizi di comunicazione elettronica, di servizi a valore aggiunto e di applicazioni di rispettare le regole, senza demonizzazioni a priori. E' però indispensabile un approccio aperto e disponibile anche da parte del mercato: la chiusura porta a sanzioni, le sanzioni sono sintomo di una sconfitta, di un fallimento sia della normativa – che non si è fatta rispettare – sia del mercato – che non ha osservato le regole. Gli operatori hanno capito che i dati personali, se trattati nel rispetto della normativa, sono asset, veri e propri forzieri di diamanti delle nuove imprese: il Garante potrebbe persino "certificare" queste ricchezze frutto di diligenza e osservanza delle leggi.

13. Come potrebbe evolversi la collaborazione attiva dei Titolari del trattamento nel perseguimento dei Reati Informatici?

Alcune recenti novità vanno nella giusta direzione: l'obbligo per i fornitori di servizi di comunicazioni elettroniche accessibili al pubblico di adottare misure di sicurezza in una logica sistemica contro possibili violazioni di dati personali, il conseguente obbligo di notificazione a Garante ed agli utenti interessati qualora tali violazioni si verifichino e, infine, l'imposizione di un modello di gestione e controllo per la tutela dei dati personali, oltre all'estensione dell'obbligo di notifica del data breach qualunque sia l'ambito di riferimento, come previsti nella proposta di Regolamento Ue.

Non ha certo senso, invece, imporre ai Titolari del trattamento una funzione di controllo preventivo sui contenuti veicolati in Rete. Inoltre, crediamo opportuna una revisione (o, almeno, una reinterpretazione) della norma penale sull'illecito trattamento dei dati, contenuta nel Codice privacy all'art. 167 e che prevale sulle esclusioni di responsabilità degli ISSP di cui al D.Lg. 70/2003: un'interpretazione troppo rigida di quell'articolo porterebbe infatti a considerare responsabili penalmente, per illecito trattamento di dati, gli amministratori dei fornitori di servizi della società dell'informazione che consentano la condivisione di contenuti generati dagli utenti sul web (motori di ricerca, social networks, ecc.). Per evitare questa forma di responsabilità penale "quasi oggettiva" in ambito informatico, i Titolari del trattamento dovrebbero filtrare e setacciare a priori i dati veicolati dagli utenti, ottenendo come risultato che – per tutelare la privacy di terzi – si violerebbe sistematicamente la privacy degli utenti di Internet. Questa precisazione sembra trovare conferma anche dalla proposta del Regolamento UE che, proprio all'art. 2, lascia

impregiudicata la disciplina della responsabilità degli ISSP dettata dalla direttiva sull'e-commerce e, quindi, dal nostro D.Lgs. 70/2003.
Quanto alla conservazione dei dati di traffico telefonico e telematico per finalità di accertamento e repressione dei reati, guardiamo favorevolmente al processo di revisione della Direttiva 2006/24/CE che si sta avviando in UE (anche grazie alle posizioni tedesche, più garantiste e attente ad evitare eccessive invasioni nella vita privata dei cittadini). In generale, non sembra ragionevole estendere ai dati di traffico che siano anche contenuti (es. indirizzi IP di destinazione) le previsioni contenute in quella normativa, sebbene si possano immaginare eccezioni subordinate a ordini delle autorità competenti per particolari categorie di delitti odiosi.

14. Il principio della "Privacy by Design": si evitino standard di Stato
Il principio della Privacy by Design è prezioso, se interpretato in modo ragionevole. Progettare le tecnologie, i prodotti e i servizi, ponendosi fin dall'inizio il problema della protezione dei dati è qualcosa di corretto e rappresenta un valore aggiunto per tutti. Due le questioni a cui fare attenzione, tuttavia: 1. non trasformare il concetto di privacy nella PBD in una sorta di "data safety", dove le scelte sono preordinate a monte come se il "data subject" andasse posto "sotto tutela": infatti dobbiamo valorizzare la libertà di scelta informata dell'utente del prodotto/servizio, senza pre-scegliere al suo posto in fase di progettazione; 2. vanno promossi standard tecnici largamente condivisi dagli operatori a livello internazionale; al fine di evitare il rischio che imposizioni dall'alto, operate dallo Stato o dalla Commissione Europea, possano alterare la concorrenza, frenando mercato e innovazione.

15. L'attuazione del nuovo obbligo di Notifica delle Violazioni all'interessato e al Garante: quali potrebbero essere i vantaggi per i Titolari che si adeguano prontamente a tale oneroso adempimento?
La notifica delle violazioni dei dati personali (come contenuta nel decreto 69/2012 di recepimento della Direttiva 2009/136/CE e, ancor più, come prevista in via generale e non settoriale nella proposta di Regolamento Ue) è una novità molto positiva che va apprezzata nel contesto generale.
Le aziende titolari di trattamento di dati personali (per ora solo se fornitrici di servizi di comunicazione elettronica) devono adottare un sistema di sicurezza idoneo ad evitare tali violazioni (il decreto 69/2012 parla di "politica di sicurezza" proprio ad indicare un approccio sistemico); qualora ciononostante si verificasse una violazione, questa andrà tempestivamente comunicata al Garante e, se particolarmente grave per i cittadini, anche a costoro.
L'informazione diretta a coloro ai quali si riferiscono i dati personali è prerequisito fondamentale per consentire a ciascuno di correre ai ripari e cercare di limitare i danni derivanti da tali violazioni nel proprio contesto di riferimento: è molto utile, ad esempio, far sì che ciascuno di noi sappia per tempo di essere stato oggetto di un "furto di dati" (potremmo bloccare la carta di credito tempestivamente, evitando frodi). L'obbligo di notificazione, pertanto, è da condividere in toto.
Di certo, la discussione si sposta poi sulla sua efficacia nell'interesse effettivo dei singoli e sulla possibile onerosità per le aziende: ma questo riguarda piuttosto le modalità attuative.

Vi sono già precedenti di modalità informative dirette ad una vasta platea di destinatari che raggiungono un giusto equilibrio nel rapporto tra onerosità ed efficacia. Sarà sufficiente farvi riferimento in modo creativo e intelligente al fine di non incorrere in soluzioni operative impraticabili o irragionevoli.
I vantaggi per i Titolari che si adeguano prontamente sono evidenti: l'obbligo di notificazione non va letto, ammesso che ciò sia possibile, come un adempimento formale. Esso costituisce il punto terminale di un processo che presuppone l'adozione di un adeguato sistema di sicurezza, un presidio organizzativo, un impianto di monitoraggio, una politica di aggiornamento ciclico. In altri termini, la notificazione tempestiva delle violazioni dei dati personali è il naturale effetto di quel modello di controllo e gestione sui dati personali prescritto dal futuro Regolamento Ue a carico di ogni azienda che ne fa uso. Visto in questa ottica, l'obbligo di notificazione abbandona l'area dell'allarmismo ed entra in una logica di operosa collaborazione tra operatori ed istituzione a beneficio della collettività. Di conseguenza, le aziende che interpretano quest'obbligo nella prospettiva qui indicata, adotteranno una politica di corretta gestione del rischio data protection a beneficio dei propri investimenti, della propria immagine e reputazione.

16. Come gestire il principio di Responsabilità (accountability) di prossima introduzione con il Regolamento Europeo

La "accountability" potrebbe essere tradotta come "responsabilità verificabile e riconducibile", nel senso inteso nel Regolamento. Questo significa che la regolamentazione dovrebbe essere meno formalistica e più concreta possibile. Si dovrà badare alla sostanza del rispetto di regole e misure di sicurezza, al di là dei pezzi di carta.
Peraltro, il nuovo principio dell'accountability in parte è già presente nel nostro ordinamento ed in parte presenta elementi di novità. Il codice privacy già impone un'inversione dell'onere della prova a carico delle aziende ed enti che sono tenuti a dimostrare "di avere adottato tutte le misure idonee a evitare il danno" derivante dal trattamento di dati personali. Ma questo profilo attualmente si gioca nell'ambito dell'azione di risarcimento danni, tra Titolare ed eventuale danneggiato e non anche come principio generale di conformità. La positiva novità del principio di "accountability" sta proprio nell'essere divenuto la chiave interpretativa del livello di conformità legale richiesto dalla norma al Titolare: questi sarà ritenuto conforme a legge se sarà "accountable" e viceversa. Ma ciò che rende ancor più innovativo il principio è la sua declinazione operativa, contenuta nella proposta di Regolamento: si è "accountable", in sintesi, solo se si adotta un adeguato modello di gestione e controllo dei dati personali fatto di ruoli e competenze, processi e procedure codificati, supervisione indipendente, valutazioni d'impatto preliminari, sanzionabilità delle violazioni, sistema di sicurezza. Un modello che ricalca quello previsto dalla normativa sulla responsabilità d'impresa per reati commessi da dipendenti o rappresentanti con tornaconto aziendale. Un modello al quale il legislatore fa spesso ricorso, essendo la migliore garanzia di effettiva conformità: anche la tutela dei dati personali si sta muovendo in questa direzione.

17. In che modo si potrebbe alleggerire l'attuale disciplina italiana in tema di fornitura di informative e richieste di consenso?

I riferimenti già fatti al bilanciamento di interessi ed ai codici deontologici sono una risposta indiretta in questo senso. Piuttosto che di alleggerimento sarebbe preferibile parlare di efficacia: in uno Stato democratico i valori fondamentali vanno tutelati anche con rimedi che, a prima vista, possono apparire onerosi, specie secondo una logica prettamente economica. Il paradosso è che talvolta questi rimedi sono onerosi e di dubbia utilità, se non addirittura vessatori per entrambe le parti coinvolte: azienda Titolare e cittadino interessato. Anche in questo contesto occorre fare un cambio di prospettiva: passare da una logica meramente prescrittiva (sancire regole fini a sé stesse) ad una strategia normativa diretta dagli obiettivi che si perseguono (si scelgono determinate regole perché risultano efficaci). Se "si gira pagina", allora diventa possibile una diversa impostazione: ci si accorge che la comunicazione testuale, ad esempio, non è più data per acquisita, come l'unica soluzione praticabile per l'informativa privacy; in quanto essa non sempre è un efficace mezzo comunicativo. Laddove lo scambio di dati è frutto di interazioni caratterizzate da velocità, bisogna ricorrere alla comunicazione per simboli, semmai corroborata da testi chiari e semplici, facilmente reperibili.
Se i soggetti che si intende tutelare sono minori, ad esempio, perché non concepire "informative a fumetti"? Abbattiamo quella barriera invisibile ma invalicabile secondo cui il messaggio normativo debba necessariamente essere aulico e difficilmente interpretabile.
Il "consenso privacy" come è stato concepito dal legislatore italiano nel codice privacy è un istituto giuridico ormai discutibile, in quanto male rappresenta quel potere di autodeterminazione informativa che ne dovrebbe essere il fondamento. Basterebbe chiedersi se, quando il cittadino acconsente all'uso dei propri dati personali, esso sia effettivamente consapevole di cosa stia dichiarando. Troppo di frequente, una volta rilasciato il consenso, l'uso dei dati è di fatto considerato legittimo, senza necessità di verificare il livello di tutela sostanziale. Quindi, da un lato il consenso rischia di non essere l'espressione di una volontà consapevole, dall'altro, non è garanzia di tutela effettiva.
Per questo, specie con l'avvento del principio di accountability di cui si è detto, il consenso potrebbe essere superato in certi casi in due direzioni: 1. con il potenziamento della cosiddetta "opposizione informata", per cui vale di più un utente veramente consapevole e in grado di bloccare un trattamento, che un utente ignaro, che non legge informative lunghissime, e che con un semplice click accetta profilazioni pesantissime e invasive; 2. con una interpretazione più elastica e meno formalistica delle modalità di espressione del consenso, che in certi casi potrebbe essere desunto dal comportamento concludente e informato dell'interessato, al di là di flag, firme, ecc.. La proposta di Regolamento Ue sembra andare in questa direzione.

18. Quali sono gli ambiti in cui la normativa Privacy andrebbe amplificata? In che modo e perché.

Nel settore pubblico e nella tutela dei minori c'è molto lavoro da fare. Ma promuovere l'ampliamento dell'ambito di applicazione normativa senza porsi preventivamente il problema della conformità e dell'efficacia, rischia di essere controproducente. Prima di pensare di ampliare occorre far rispettare la norma vigente, in una logica efficace per i valori tutelati.
In linea generale, infatti, si avverte l'esigenza di una maggiore efficacia della normativa privacy piuttosto che di una sua amplificazione. Prevedere adempimenti che non portano a

concrete salvaguardie ma che, piuttosto, denotano burocratici impedimenti alla normale gestione delle attività di impresa, scontenta sia i soggetti destinatari (aziende ed enti) sia i potenziali beneficiari (consumatori, utenti e cittadini in genere).
In questo ambito, forse più che in altri, occorre sempre fare una valutazione preventiva di impatto della regolazione che si propone di introdurre così come sarebbe opportuno ricorrere alla pratica della preliminare consultazione pubblica sulle proposte normative. Si è detto in altra sede che il ricorso ai codici deontologici previsti dal codice privacy può essere una valida soluzione per esigenze sia di ampliamento che di efficacia.

19. Qual è il punto di vista dell'Istituto Italiano per la Privacy sulla probabile evoluzione e sullo sfruttamento di quello che chiamano Big Data (nel senso di analisi, aggregazione delle informazioni)?
L'economia digitale non si limita al web, ma coinvolge televisioni, internet delle cose, reti elettriche intelligenti, geo-referenziazione e realtà aumentata, servizi socio-sanitari, e molto altro ancora. C'è una enorme massa di dati – anche personali – che sono elaborabili dalle imprese per fornire servizi avanzatissimi o per mirare pubblicità sempre più pertinente e personalizzata: quanto più massivo è il quantitativo di dati personali raccolto ed elaborabile, tanto più completa ed analitica deve essere la disciplina di tutela di tali informazioni a protezione degli individui ai quali esse si riferiscono. Come sarebbe illusorio immaginare di frenare la tendenza ad un intenso sfruttamento delle informazioni personali, così altrettanto insana sarebbe l'elusione di una protezione sostanziale degli utenti-consumatori interessati: è indispensabile, quindi, aumentare esponenzialmente i diritti e i poteri degli utenti, imporre la massima trasparenza agli operatori, fare in modo che il dominio sui propri dati, da parte degli interessati, sia totale e libero, flessibile e sicuro. Ci preoccupano maggiormente gli usi di Big Data da parte di soggetti pubblici, anche di altri Paesi, senza trasparenza né adeguate garanzie per i cittadini.

www.istitutoitalianoprivacy.it