CONSUMERS' FORUM

in collaborazione con: help consumatori

Obiettivo Europa

Newsletter sul semestre di Presidenza italiana del Consiglio dell'Unione europea

inserto della newsletter Dialogo Aperto

n. 3

Privacy, l'Europa di fronte alla sfida della protezione dei dati

Conservazione dei dati e diritto all'oblio: le sentenze della Corte di Giustizia

A che punto è la riforma della protezione dei dati? Parla la Portavoce della Commissione per la Giustizia, i diritti fondamentali e la cittadinanza, Mina Andreeva

L'Italia non resta a guardare

Che ruolo giocherà l'Italia durante il semestre europeo? Intervista al Garante Privacy Antonello Soro

I principali interventi del Garante Privacy nei primi 6 mesi del 2014

Street View viola la privacy, maxi multa per Google

Obiettivo Europa

Newsletter sul semestre di Presidenza italiana del Consiglio dell'Unione europea

inserto della newsletter Dialogo Aperto

n. 3

Privacy, l'Europa di fronte alla sfida della protezione dei dati

Il 2014 è un anno cruciale per la privacy dei cittadini europei. Le istituzioni comunitarie stanno ragionando da tempo su come aggiornare al meglio le norme sulla protezione dei dati personali che attualmente risalgono al 1995, praticamente alla preistoria dell'era digitale. Basti pensare che in quell'anno il fondatore di Facebook aveva appena 11 anni ed era impossibile immaginare la diffusione capillare che avrebbero avuto smartphone e social network. Oggi chi usa uno smartphone ha in media 40 applicazioni in grado di raccogliere e diffondere dati sensibili**. Le informazioni personali sono ormai la moneta dell'economia digitale**: interi modelli di business si fondano sullo scambio di dati e un recente studio ha stimato il valore del mercato europeo dei dati personali in 50 miliardi di euro. Cifra che potrebbe crescere in modo più che esponenziale, arrivando quest'anno addirittura a 350 miliardi. La domanda delle domande è: **cosa vuol dire, nell'era digitale, tutelare il diritto alla privacy?** Non si tratta più del semplice rispetto della riservatezza della sfera personale; oggi si fa riferimento ad un diritto più ampio che ognuno di noi dovrebbe avere sulla diffusione e sull'utilizzo di tutte le informazioni che riguardano la propria persona. Una materia tanto delicata quanto fondamentale: le nuove tecnologie aprono continuamente nuovi scenari che a volte sono sconosciuti agli stessi operatori del settore. Non possiamo quindi accontentarci di norme così vecchie. L'Europa deve trovare presto un accordo su nuove leggi per la protezione dei dati.

Due anni fa la Commissione Europea ha proposto una riforma radicale e gli Stati membri stanno ragionando attorno ad essa per arrivare all'approvazione. Ad ottobre 2013 la Commissione per le libertà civili, la giustizia e gli affari interni (LIBE) del Parlamento europeo ha votato a larga maggioranza a favore delle proposte della Commissione e nel frattempo ne ha discusso anche il Consiglio "Giustizia e affari interni". Ma il passo più importante è stato fatto il 12 marzo dai deputati europei in Plenaria che, a larga maggioranza, hanno votato a favore della riforma proposta dalla Commissione Europea rafforzando ulteriormente l'architettura sia della direttiva sia del regolamento, che costituiscono il pacchetto di riforma sulla protezione dei dati.

In occasione della Giornata europea della protezione dei dati, che si celebra ogni anno il 28 gennaio, la Rappresentanza in Italia della Commissione UE ha organizzato un convegno molto interessante durante il quale il Vicecapo Unità Protezioni dei dati personali della Direzione generale Giustizia della Commissione UE, Bruno Gencarelli, ha ricordato gli elementi centrali della riforma:

- **maggiore armonizzazione e semplificazione della disciplina**, che permetterà di superare l'attuale frammentazione del mercato, gli alti costi e i tempi lunghi imposti alle imprese. Grazie al meccanismo dello "sportello unico" (detto *one-stop-shop*) ogni operatore dovrà essere soggetto alla vigilanza di un'unica autorità garante per qualsiasi operazione riguardante i dati personali;

- **potenziamento degli aspetti normativi di vigilanza**, che prevedono sanzioni fino al 2% del fatturato della società che ha violato la privacy;

- **rafforzamento dei diritti dei cittadini**: accanto a quelli tradizionali, si prevedono una serie di strumenti innovativi per garantire il diritto all'oblio, una maggior tutela dei minori, il diritto alla portabilità dei dati (come nel caso della telefonia), e una tempestiva informazione agli interessati in caso di accesso illegittimo ai dati.

Obiettivo Europa
Newsletter sul semestre di Presidenza italiana del Consiglio dell'Unione europea
inserto della newsletter Dialogo Aperto
n. 3

Per accelerare i tempi di approvazione della riforma, la Commissaria europea per la Giustizia **Viviane Reding ha proposto un "Patto di protezione dei dati personali per l'Europa"** fondato su 8 principi, tra cui il fatto che i dati dovrebbero essere raccolti in modo mirato e limitatamente a quanto proporzionato per il conseguimento delle finalità previste (la sorveglianza totale e indiscriminata dei dati delle comunicazioni elettroniche è inaccettabile) e che la sicurezza nazionale non è una motivazione che si possa addurre ad ogni piè sospinto (dovrebbe essere l'eccezione, non la regola). Infine, un messaggio agli americani: le norme sulla protezione dei dati personali dovrebbero applicarsi quale che sia la cittadinanza dell'interessato; dato il carattere aperto di internet, non ha senso applicare ai cittadini degli altri paesi criteri diversi rispetto ai propri cittadini.

L'Italia potrà giocare un ruolo decisivo nella approvazione della riforma sulla privacy: prima di tutto perché il nostro Paese ha un Codice della privacy molto avanzato, considerato un modello in Europa, e poi perché dal 1° luglio l'Italia è alla guida del semestre europeo. La presidenza greca del primo semestre ha già inserito l'adozione della riforma nella tabella di marcia, ed è molto probabile che entro la fine del 2014 si raggiungerà l'obiettivo.

Conservazione dei dati e diritto all'oblio: le sentenze della Corte di Giustizia

Ci sono una serie di fatti accaduti in questi primi sei mesi dell'anno, che non potranno essere lasciati da parte. Prima di tutto c'è stata **una sentenza della Corte di Giustizia dell'Unione Europea che ha dichiarato invalida la direttiva comunitaria sulla conservazione dei dati** (generati o trattati da fornitori di servizi di comunicazioni elettroniche accessibili al pubblico o di una rete pubblica di comunicazioni). Il motivo? Comporta un'ingerenza di vasta portata e particolare gravità (non limitata allo stretto necessario) in due diritti fondamentali: il rispetto della vita privata e la protezione dei dati di carattere personale. I dati da conservare consentono di sapere con quale persona e con quale mezzo un abbonato o un utente registrato ha comunicato, di determinare il momento della comunicazione e il luogo da cui ha avuto origine e di conoscere la frequenza delle comunicazioni dell'abbonato o dell'utente registrato con determinate persone in uno specifico periodo. **Secondo i giudici europei tali dati, considerati congiuntamente, possono fornire indicazioni assai precise sulla vita privata dei soggetti** i cui dati sono conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri o di diversa frequenza, le attività svolte, le relazioni sociali e gli ambienti sociali frequentati. La direttiva, inoltre, si applica all'insieme degli individui, dei mezzi di comunicazione elettronica e dei dati relativi al traffico, senza che venga operata alcuna differenziazione, limitazione o eccezione in ragione dell'obiettivo della lotta contro i reati gravi. La Corte ha anche contestato il fatto che la direttiva non impone che i dati siano conservati sul territorio dell'UE, non garantendo, quindi, il pieno controllo da parte di un'autorità indipendente del rispetto delle esigenze di protezione e di sicurezza. **Il Presidente dell'Autorità Garante per la privacy italiana, Antonello Soro, ha commentato positivamente la sentenza che "va nella direzione auspicata di una più marcata tutela dei diritti, riequilibrando due valori, sicurezza e privacy, che in questi anni si erano decisamente disallineati".** Soro ha sottolineato: "I dati di traffico non sono informazioni neutre ma rivelano molto della vita privata di tutti noi. Un'indifferenziata conservazione

di questi dati per periodi molto lunghi espone quindi a grandi rischi. Inoltre la Corte ha sottolineato l'esigenza che i dati oggetto di conservazione per ragioni di giustizia restino nel territorio dell'Ue con evidente riferimento alle note vicende del Datagate. Occorrerà una revisione dell'attuale sistema nel segno del principio di proporzionalità e delle garanzie per i cittadini".

Ma c'è un'altra sentenza della **Corte di Giustizia dell'UE** **che è intervenuta su questi temi, in particolare sul diritto all'oblio**. La Corte ha affermato la responsabilità del gestore di un motore di ricerca sul trattamento da esso effettuato dei dati personali che appaiono su pagine pubblicate da terzi. In pratica se facendo una ricerca sul nostro nome, ad esempio su Google, troviamo tra i risultati dei link a pagine web che contengono informazioni su di noi che non ci piacciono (perché violano il nostro diritto fondamentale alla vita privata), possiamo chiedere che quei link vengano rimossi. Secondo la Corte il gestore del motore di ricerca è il responsabile del trattamento dei dati perché è lui a determinarne le finalità e gli strumenti del trattamento stesso. Si tratta, infatti, di dati che toccano potenzialmente una moltitudine di aspetti della vita privata e che, in assenza del motore di ricerca, difficilmente avrebbero potuto essere connesse tra loro. **Gli utenti di Internet possono così stabilire un profilo più o meno dettagliato delle persone ricercate.** Bisogna quindi cercare un equilibrio tra i diritti al rispetto della vita privata e alla protezione dei dati personali e il legittimo interesse degli utenti di Internet ad alcune informazioni. Equilibrio che dipende sicuramente dalla natura dell'informazione pubblicata e dal suo carattere sensibile per la vita privata della persona coinvolta, ma anche dall'interesse del pubblico a ricevere tale informazione, il quale può variare a seconda del ruolo che tale persona riveste nella vita pubblica.

Sulla questione del diritto all'oblio (ovvero sul diritto della persona interessata di chiedere che dei link verso pagine web siano cancellati dall'elenco di risultati per il fatto che questa persona desideri che le informazioni relative alla sua persona siano oggetto di "oblio" dopo un certo tempo), **la Corte rileva che, qualora si constati, in seguito a una richiesta dell'interessato, che l'inclusione di tali link nell'elenco è, allo stato attuale, incompatibile con la direttiva, le informazioni e i link figuranti in tale elenco devono essere cancellati.** L'utente può rivolgersi direttamente al gestore del motore di ricerca, che deve prendere in esame la fondatezza della richiesta. In seconda battuta può rivolgersi all'autorità di controllo o giudiziaria.

Lasciando tutti un po' di "sorpresa", a pochi giorni da questa sentenza, Google si è subito adeguato alle indicazioni ed ha lanciato il servizio per far valere il "diritto all'oblio". Compilando un modulo messo a disposizione dal colosso del web, tutti gli utenti possono chiedere la rimozione di link che appaiono dopo una ricerca sul proprio nome, qualora contengano informazioni "inadeguate, irrilevanti o non più rilevanti, o eccessive in relazione agli scopi per cui sono stati pubblicate". Sarà Google a valutare "ogni singola richiesta", cercando di "bilanciare i diritti sulla privacy della persona con il diritto di tutti di conoscere e distribuire le informazioni", riservandosi il compito di stabilire "se i risultati includono informazioni obsolete sull'utente e se le informazioni sono di interesse pubblico, ad esempio se riguardano frodi finanziarie, negligenza professionale, condanne penali o la condotta pubblica di funzionari statali. La mossa di Google di adeguarsi all'ordinamento europeo è stata accolta da tutti come "un fatto positivo", sulla cui corretta applicazione bisogna, però, verificare. In questo senso, resta di grande importanza il ruolo che potranno svolgere le Autorità nazionali per la privacy, con le quali deve proseguire il proficuo lavoro comune e coordinato già avviato proprio nei confronti di Google e degli altri Big della Rete.

Obiettivo Europa
Newsletter sul semestre di Presidenza italiana del Consiglio dell'Unione europea
inserto della newsletter Dialogo Aperto
n. 3

A che punto è la riforma della protezione dei dati? Parla la Portavoce della Commissione per la Giustizia, i diritti fondamentali e la cittadinanza, Mina Andreeva

A che punto è la riforma sulla protezione dei dati personali? Quali sono i principali ostacoli alla sua approvazione?

"Il 25 gennaio 2012 la Commissione Europea ha presentato una riforma completa di tutto il contesto europeo della protezione dei dati. Il pacchetto di riforme consiste in un Regolamento che disegna un quadro generale, rafforzando il diritto alla protezione dei dati in linea con la Carta Europea dei Diritti Fondamentali, e in una Direttiva che si applicherà ai processi di protezione dei dati, sia nazionali che transnazionali, gestiti dalle autorità di polizia e di giustizia. L'obiettivo è quello di superare l'attuale mosaico di normative nazionali differenti e, nello stesso tempo, ridurre gli oneri a carico delle imprese generando, ogni anno, un risparmio di circa 2,3 miliardi di euro.

Riteniamo che sia stato un momento molto importante il voto del Parlamento Europeo dello scorso 12 marzo, espresso al larga maggioranza a favore della riforma della Commissione Europea. Il Parlamento ha dato il suo grande contributo all'architettura ed ai principi fondamentali della proposta della Commissione, rafforzando il contesto legislativo sia della Direttiva che del Regolamento. Il voto in Plenaria ha reso la riforma sulla protezione dei dati irreversibile ed ha blindato la posizione del Parlamento Europeo, anche rispetto alla nuova composizione dell'Aula a seguito delle elezioni europee. Un altro balzo in avanti è stato compiuto durante il Consiglio Giustizia di giugno, quando i Ministri della Giustizia hanno raggiunto l'accordo su due importanti pilastri della riforma della protezione dei dati: sulle regole che dovranno governare il trasferimento dei dati ai paesi terzi e sugli ambiti territoriali della regolazione sulla protezione dei dati. In poche parole: la legislazione europea sulla protezione dei dati si applicherà alle società non europee se queste faranno i loro affari sul nostro territorio, all'interno del mercato unico europeo.

Gli Stati membri hanno anche espresso una posizione comune sul principio dello sportello unico (one-stop-shop) che prevede che venga adottata un'unica decisione, presa da un'unica autorità di regolazione, nei servizi transfrontalieri che gestiscono dati personali. Questo meccanismo taglierà i passaggi burocratici per le aziende e per i cittadini e darà certezza di applicazione delle regole sulla protezione dei dati all'interno dell'Unione Europea. Le diverse posizioni stanno convergendo su un modello che prevede un'autorità capo che lavora a stretto contatto con le altre autorità locali, più vicine ai cittadini, per assicurare così il principio di prossimità.

In breve: la riforma sulla protezione dei dati procede spedita ed è sulla strada giusta per assicurare il compimento del mercato unico digitale nel 2015, obiettivo fissato dai Capi di Stato ad ottobre 2013. Concretamente questo vuol dire che i negoziati si stanno intensificando con la velocità necessaria, in vista di una possibile conclusione della discussione durante la Presidenza italiana che guida il semestre europeo da luglio 2014.

Come si può contrastare lo strapotere dei giganti della rete? Bisogna agire più sul piano economico, cercando di risolvere il problema della fiscalità delle Big Companies, oppure su quello dei diritti e dell'etica?

La riforma sulla protezione dei dati non è semplicemente una questione che riguarda le Big Companies. Il suo obiettivo principale è quello di rafforzare il di-

ritto individuale alla protezione dei dati (soprattutto online) e, nello stesso tempo, facilitare le imprese (piccole e grandi) a lavorare ed investire all'interno del mercato europeo, promuovendo così la nostra economia digitale. Questo contribuirà anche a rafforzare la fiducia dei consumatori nei servizi online e tutti sappiamo che una maggior fiducia si traduce direttamente in maggiori guadagni per le aziende che gestiscono le informazioni dei cittadini. Nuovi diritti, come quello all'oblio e alla portabilità dei dati, sono cruciali per assicurare che i cittadini si sentano sicuri ed abbiamo sotto controllo i propri dati.

Oggi la maggior parte delle autorità di protezione dei dati non hanno il potere di sanzionare le violazioni delle leggi sulla privacy oppure le sanzioni che possono imporre sono così basse che i trasgressori non hanno alcuna difficoltà a pagarle e si prendono gioco delle leggi, continuando a violarle. Nessuno può pensare seriamente che questa situazione continui. Le sanzioni per violazione della privacy devono essere effettive e dissuasive, altrimenti non potranno avere alcun potere deterrente. Le violazioni delle regole sulla privacy possono portare alti profitti alle società e questo vuol dire che deve esserci una relazione diretta tra i benefici derivanti da queste violazioni e l'ammontare delle sanzioni. Nella sua riforma la Commissione Europea ha proposto multe fino al 2% del giro d'affari totale delle imprese. Proposta che è stata ulteriormente rafforzata dal Parlamento Europeo che ha votato per innalzare la soglia al 5%. Le nuove regole mantengono lo stesso principio che viene applicato quando si calcolano le sanzioni in altri settori legali, ma in questo caso la cifra dipenderà da profitti ottenuti illegalmente.

Qual è la strategia europea in materia di Big Data il cui mercato, si stima, raggiungerà il valore di 17 miliardi di dollari nel 2015?

Il diritto fondamentale alla protezione dei dati si applica ai Big Data quando i dati trattati sono personali: quindi le regole europee sulla protezione dei dati si applicano ai Big Data. Questi richiedono una grande fiducia e il pacchetto di riforma sulla protezione dei dati proposta dalla Commissione Europea mira a costruire un quadro unico, moderno, forte e completo per l'Unione Europea. Rafforzando la sicurezza individuale e la fiducia nei mercati digitali e migliorando la certezza del diritto, si creerà un contesto di regolazione essenziale per lo sviluppo di processi innovativi e sostenibili sui dati personali, che comprendono l'introduzione del diritto alla portabilità dei dati personali e ad una maggiore trasparenza. Sono incluse particolari disposizioni che si adattano all'ambiente dei Big Data. La Commissione Europea ha inoltre adottato una strategia per "liberare il potenziale del Cloud Computing in Europe", elaborata per accelerare e migliorare l'uso del cloud computing in tutti i settori economici, attraverso la realizzazione di azioni importanti ed urgenti. Tuttavia, su richiesta del Consiglio Europeo, la Commissione lavorerà sulle linee guida per un'azione europea che tenga conto delle giuste condizioni per un mercato unico dei Big Data e del cloud computing.

Cosa può fare oggi il cittadino europeo per difendere la sua privacy?

I cittadini europei godono già di uno dei contesti legali sulla privacy tra i più avanzati al mondo, orientato alla protezione delle loro informazioni personali. Se, per esempio, un cittadino dell'UE crede che il proprio diritto fondamentale alla protezione dei dati sia stato violato può inviare una segnalazione all'autorità nazionale della privacy che può, dopo un attento esame del caso, adottare misure concrete per mettere fine alla violazione in questione, compresa l'applicazione di una sanzione. I cittadini europei possono, inoltre, adire i tribunali nazionali per sostenere i propri diritti alla protezione dei dati, garantiti dalle leggi nazionali ed europee. Ancora, un cittadino europeo può chiedere che i propri dati personali vengano cancellati se questi dati non sono più necessari. Questo principio

è stato di recente ribadito dalla sentenza della Corte di Giustizia dell'UE contro Google. La decisione della Corte dimostra chiaramente che il principio del diritto all'oblio necessita di essere aggiornato e chiarito in un'epoca digitale. La proposta di regolamento sulla protezione dei dati rafforza questo principio e migliora la certezza delle regole per aziende e cittadini. Vorrei invitare i cittadini ad andare a dare un'occhiata alla scheda che abbiamo preparato a seguito della recente decisione della Corte di Giustizia sul diritto all'oblio e che è allegata alla sentenza.

L'Italia non resta a guardare

Il presidente dell'Autorità per la privacy italiana, Antonello Soro, nella sua relazione annuale, non a caso intitolata "Big data e sorveglianza globale", ha sottolineato come nella società digitale "tutto ruoti intorno alla profilazione, sempre più individualizzata e pervasiva" (siamo tutti perennemente connessi e perfettamente profilati, spesso inconsapevolmente). In questo contesto la tutela della privacy riveste un'importanza ancora più forte in quanto le grandi aziende hanno "un patrimonio informativo immenso" e questo attribuisce loro un grande potere, sottratto a regole democratiche. E se "il Datagate ha rappresentato un punto di non ritorno nel rapporto tra privacy e sicurezza", per cui "difendere la privacy significa anzitutto difendere la libertà", le attività di spionaggio informatico hanno messo in evidenza anche "l'intreccio pericoloso" che si può realizzare fra aziende digitali e spionaggio. Oggi il potere delle aziende è direttamente proporzionale al patrimonio informativo di cui dispongono, ma in mezzo ci sono i giganti della rete che tendono ad occupare, in modo sempre più esclusivo, ogni spazio di intermediazione tra produttori e consumatori, assumendo un potere (in primis quello di indirizzare le nostre decisioni) che inesorabilmente si traduce in forza politica, sottratta a qualunque regola democratica.

Per non parlare delle nuove forme di criminalità che maturano in rete, dal furto di identità alla più organizzata criminalità cibernetica: un'emorragia stimata in 500 miliardi di dollari l'anno tra identità violate, segreti aziendali razziati, portali messi fuori uso e moneta virtuale sottratta. Poi ci sono i casi sempre più frequenti di incitamento all'odio e di cyberbullismo, che colpiscono, dietro "l'infondata presunzione di anonimato", le persone più vulnerabili: si tratta di fenomeni in cui la repressione non basta. Infatti l'attività del Garante è orientata a promuovere tra i giovani una cultura della "cittadinanza digitale", che non li consideri solo come consumatori passivi di tecnologia, ma li incoraggi a comprendere gli effetti e i rischi di un uso troppo disinvolto o distorto della Rete. In questo la scuola svolge un ruolo centrale e Soro ha anche proposto di introdurre già dalle elementari l'educazione digitale come materia di studio: un'estensione dell'educazione civica, che dia una formazione appropriata dei profili etici e tecnici delle tecnologie digitali. Capitolo a parte per i social network, sul cui uso consapevole il Garante ha pubblicato la guida "Social Privacy – Come tutelarsi nell'era dei social network": un vademecum con una serie di consigli e soluzioni per non cadere nei numerosi rischi che si celano dietro queste piattaforme.

Obiettivo Europa

Newsletter sul semestre di Presidenza italiana del Consiglio dell'Unione europea

inserto della newsletter Dialogo Aperto

n. 3

Che ruolo giocherà l'Italia durante il semestre europeo? Intervista al Garante Privacy Antonello Soro

A che punto è la cultura della privacy in Italia?

"Il caso Datagate e le rivelazioni di Snowden hanno posto con forza al centro dell'attenzione anche dell'opinione pubblica italiana il tema della privacy. Nella nostra società sta crescendo la preoccupazione per i rischi a cui sono soggetti i dati personali e la necessità che essi vengano protetti perché rappresentano la nostra identità. E oggi che le persone trascorrono molto più tempo nello spazio digitale che in quello fisico, proteggere i dati personali sulla rete significa proteggere la nostra stessa vita. Tuttavia, a fronte della percezione dei rischi connessi all'uso delle reti, i cittadini italiani appaiono scarsamente in grado di mettere in atto misure e accorgimenti per tutelare i propri dati e di adottare una *gestione attiva della privacy*. E' sempre più necessario, dunque, insieme al lavoro di regolazione e vigilanza, realizzare una forte azione di sensibilizzazione. Su questo fronte il Garante è impegnato da tempo".

Cosa può fare, durante la guida del semestre europeo, il Governo italiano per accelerare l'approvazione della riforma della direttiva sulla protezione dei dati personali? Quali sono i principali ostacoli alla sua approvazione?

"Stiamo attraversando una fase importante per la tutela della privacy, nei confronti della quale si sta avvertendo un cambiamento importante da parte della giurisprudenza europea, delle aziende e dell'opinione pubblica. Basti pensare alle recenti decisioni della Corte di Giustizia dell'Unione Europea: la prima, di aprile, sul mancato bilanciamento tra il diritto alla privacy e quello alla sicurezza in materia di data retention; la seconda, di maggio, sul riconoscimento del diritto all'oblio. Le aziende, da parte loro, temendo una perdita di fiducia da parte dei consumatori, cominciano a mostrarsi disponibili a confrontarsi sull'acquisizione del consenso e su come rendere informative più dettagliate e trasparenti sugli scopi per i quali usano i dati degli utenti. In questo contesto, è necessario dunque che anche la politica faccia la sua parte. Il mio auspicio è che i governi prendano iniziative e investano in maniera decisa nella protezione dei dati. Il semestre di presidenza italiano appena cominciato può essere una occasione importante per mettere la "questione privacy" al centro dell'azione dell'Unione. E procedere, in particolare, ad accelerare il processo di adozione del nuovo Regolamento europeo in materia di protezione dei dati personali".

Come si può contrastare lo strapotere dei giganti della rete? Bisogna agire più sul piano economico, cercando di risolvere il problema della fiscalità delle Big Companies, oppure su quello dei diritti e dell'etica?

"I giganti di Internet, mentre offrono agli utenti servizi gratuiti in cambio di un massiccio prelievo di dati e informazioni, tendono ad occupare ogni spazio di intermediazione tra produttori e consumatori. E' evidente che, dal punto di vista economico, lo sviluppo della società digitale comporta problemi di natura fiscale. Quel che è certo è che si è aperta una fase nuova, che spinge tutti ad affrontare le contraddizioni della Rete e a ricercare ulteriori equilibri tra fattibilità tecnica, accettabilità giuridica e fondamento etico della società digitale. Il compito dell'Autorità Garante per la protezione dei dati personali è di farsi carico di tutelare il versante dei diritti, perché non può esistere un'Europa dell'economia senza un'Europa dei diritti".

Oggi il consumatore/cittadino europeo ha un diritto in più, quello all'oblio. Qual è il suo parere?

"In Europa le garanzie a tutela dei cittadini sono numerose e consolidate. A queste si è aggiunta di recente quella al diritto all'oblio a cui ha dato concreto riconoscimento la recente sentenza della Corte di Giustizia che ricordavo prima quando stabilito che i motori di ricerca sono comunque responsabili del trattamento dei dati personali reperiti su siti Internet gestiti da terzi. Qualora, dunque, un cittadino volesse ottenere la deindicizzazione di informazioni che lo riguardano, può rivolgersi direttamente al motore di ricerca. E' vero tuttavia, e lo si vede dal recente caso relativo ad un banchiere, che l'applicazione effettiva di questo diritto pone non pochi problemi. Occorre garantire il bilanciamento tra il diritto all'oblio e quello all'informazione e non credo che Google possa operarlo da sola. E' necessario trovare meccanismi attraverso i quali affermare il ruolo delle Autorità di garanzia, ruolo che è e rimane imprescindibile".

I principali interventi del Garante Privacy nei primi 6 mesi del 2014

OFFERTE TELEFONICHE E PROFILAZIONE: sono sempre di più gli utenti che ricorrono alla "number portability", che permette di cambiare fornitore del servizio in poco tempo (anche in un giorno) conservando lo stesso numero di telefono ed inseguendo l'offerta più vantaggiosa. Per consentire agli operatori una più corretta e puntuale offerta alla clientela, il Garante ha aggiornato le regole che le società telefoniche sono tenute a seguire nelle attività di profilazione: le società potranno analizzare in 2 giorni anziché in un mese alcune categorie di dati aggregati, come il volume di minuti in traffico originato o terminato (in minuti o byte); il numero di ricariche (distinto per canale di acquisto: online, bancomat, carte prepagate); il totale delle ricariche. Le società dovranno escludere dall'esame i dati riferibili ad un solo evento di comunicazione effettuato da un singolo utente. Restano inalterate le garanzie già fissate a tutela dei clienti, che prevedono, tra l'altro, l'impiego di sistemi informatici dedicati alla profilazione separati da quelli utilizzati per altre finalità (ad es. fatturazione e marketing) e l'adozione di rigorose misure di protezione per l'accesso ai dati, con procedure di autenticazione individuali e profili differenziati rispetto a quelli richiesti per l'accesso ad altri sistemi aziendali.

TELEMARKETING AGGRESSIVO, ovvero quella forma di marketing, percepita quasi come persecuzione, per cui l'utente riceve diverse telefonate che dovrebbero essere pubblicitarie, invece sono "mute". La telefonata muta è frutto delle impostazioni dei sistemi centralizzati di chiamata dei call center, che vogliono massimizzare la produttività degli operatori. Sono numerosi gli abbonati che hanno segnalato al Garante la ricezione di questo tipo di telefonate anche per 10-15 volte di seguito. Dopo una consultazione pubblica durata un anno, è stato varato un provvedimento che impone agli operatori di adottare misure specifiche per ridurre questo disturbo. Prima di tutto, i call center dovranno tenere precisa traccia delle "chiamate mute", che dovranno comunque essere interrotte trascorsi 3 secondi dalla risposta dell'utente**.** Non potranno verificarsi più di 3 telefonate "mute" ogni 100 andate "a buon fine". L'utente non dovrà essere messo in attesa silenziosa, ma il sistema dovrà creare un rumore ambientale di fondo per dare la sensazione che la chiamata provenga da un call center e non da un eventuale molestatore. Ancora: l'utente disturbato da una telefonata muta non potrà essere ricontattato per 5 giorni e, al contatto successivo, dovrà parlare un operatore. I call center dovranno infine conservare per almeno 2 anni

i report statistici delle telefonate "mute" effettuate per ciascuna campagna, così da consentire eventuali controlli.

COOKIES. Stop all'installazione dei cookie per finalità di profilazione e marketing da parte dei gestori dei siti senza aver il consenso informato degli utenti. Chi naviga online potrà decidere in maniera libera e consapevole se far usare o no le informazioni raccolte sui siti visitati per ricevere pubblicità mirata. Lo ha stabilito il Garante privacy con un provvedimento adottato al termine di una consultazione pubblica. Per proteggere la privacy degli utenti e consentire loro scelte più consapevoli, il Garante ha stabilito che, d'ora in poi, quando si accede alla home page o ad un'altra pagina di un sito web deve immediatamente comparire un banner ben visibile, in cui sia indicato chiaramente:

1. che il sito utilizza cookie di profilazione per inviare messaggi pubblicitari mirati;
2. che il sito consente anche l'invio di cookie di "terze parti", ossia di cookie installati da un sito diverso tramite il sito che si sta visitando;
3. un link a una informativa più ampia, con le indicazioni sull'uso dei cookie inviati dal sito, dove è possibile negare il consenso alla loro installazione direttamente o collegandosi ai vari siti nel caso dei cookie di "terze parti";
4. l'indicazione che proseguendo nella navigazione (ad es., accedendo ad un'altra area del sito o selezionando un'immagine o un link) si presta il consenso all'uso dei cookie.

Per quanto riguarda l'obbligo di tener traccia del consenso dell'utente, al gestore del sito è consentito utilizzare un cookie tecnico, in modo tale da non riproporre l'informativa breve alla seconda visita dell'utente. L'utente mantiene, comunque, la possibilità di modificare le proprie scelte sui cookie attraverso l'informativa estesa, che deve essere linkabile da ogni pagina del sito.

MOBILE PAYMENT. Il Garante ha adottato nuove regole sul mobile payment, a tutela della privacy di chi fa acquisti pagando con il proprio smartphone o tablet: i dati personali acquisiti per la transazione (numero telefonico, dati anagrafici, informazioni sul servizio o prodotto richiesto, indirizzo IP) non potranno essere usati per altre finalità, come l'invio di pubblicità o analisi delle abitudini, senza lo specifico consenso degli utenti, e dovranno essere protetti dai rischi di uso fraudolento. **Informativa:** gli utenti dovranno essere informati sulle modalità di trattamento effettuato sui loro dati sin dalla sottoscrizione o adesione al servizio di pagamento da remoto. **Consenso:** le società non dovranno richiedere il consenso degli utenti per il trattamento dei dati relativi alla fornitura del servizio di remote mobile payment. Il consenso è invece obbligatorio per la comunicazione dei dati personali a terzi oppure in caso di loro utilizzo per attività di marketing e profilazione. **Conservazione:** i dati degli utenti trattati dagli operatori, dagli aggregatori e venditori, potranno essere conservati al massimo per 6 mesi**.** L'indirizzo Ip dell'utente dovrà invece essere cancellato dal venditore una volta terminata la procedura di acquisto del contenuto digitale. **Misure di sicurezza:** operatori, aggregatori e venditori saranno tenuti ad adottare precise misure per garantire la confidenzialità dei dati, ad esempio sistemi di autenticazione per l'acceso ai dati da parte del personale addetto, procedure di tracciamento degli accessi e delle operazioni effettuate; criteri di codificazione dei prodotti e servizi; forme di mascheramento dei dati mediante sistemi crittografici; misure che impediscono l'integrazione delle diverse tipologie di dati a disposizione dell'operatore telefonico (dal consumo telefonico ai dati sull'uso della tv interattiva) ed evitano la profilazione "incrociata" dell'utenza basata su abitudini, gusti e preferenze, a meno che non venga espresso uno specifico consenso informato da parte dell'utente. Dovranno essere previsti anche accorgimenti tecnici per disattivare servizi destinati ad un "pubblico adulto" e per inibirne l'accesso a minorenni.

Obiettivo Europa
Newsletter sul semestre di Presidenza italiana del Consiglio dell'Unione europea
inserto della newsletter Dialogo Aperto
n. 3

Street View viola la privacy, maxi multa per Google

Anche il 2013 è stato un anno cruciale per la privacy: sono stati 606 i provvedimenti collegiali adottati dal Garante, 222 i ricorsi decisi, relativi soprattutto a banche e società finanziarie, attività di marketing, compagnie di assicurazione, operatori telefonici e telematici. L'Autorità nel suo complesso ha fornito a Governo e Parlamento 22 pareri ed effettuato 411 ispezioni (+4% rispetto al 2012) su settori diversi, dai call center alle banche dati del fisco, dai nuovi strumenti di pagamento gestiti dalle compagnie telefoniche (mobile payment) alle violazioni delle banche dati dei gestori delle telecomunicazioni (i data breaches). Il Garante Privacy ha contestato 850 violazioni amministrative e deciso sanzioni per oltre 4 milioni di euro.

Ma il provvedimento che ha fatto più scalpore è stata **la maxi multa, da un milione di euro, inflitta a Google** a dicembre 2013 per violazione della privacy attraverso il servizio **Google Street View**. Nell'ordinanza di ingiunzione il Garante ha contestato a Google la violazione delle norme del Codice della Privacy "concernente l'inidoneità dell'informativa resa agli interessati con riferimento ad una banca dati di particolari dimensioni in occasione della raccolta di dati effettuata dalla società mediante le cosiddette Google cars nell'ambito del servizio denominato Street View". Il servizio rappresenta un'evoluzione di Google Maps che permette di avere immagini dettagliatissime delle città attraverso fotografie panoramiche scattate al livello della strada. Volti e targhe delle automobili sono oscurati ma questo non impedisce, in realtà, di riconoscere vetture o di ritrovarsi immortalati per lungo tempo nelle fotografie scattate in strada.

I fatti contestati risalgono al 2010 quando le auto del colosso di Mountain View hanno percorso le strade italiane senza essere perfettamente riconoscibili e non consentendo, in tal modo, alle persone presenti nei luoghi percorsi di decidere se sottrarsi o meno alla "cattura" delle immagini. Numerose erano state le segnalazioni all'Autorità da parte di persone che non desideravano comparire nelle foto pubblicate online (che, peraltro, permangono in rete per un tempo considerevole e possono essere ingrandite). Il Garante aveva prescritto alla società di rendere le "Google cars" facilmente individuabili, attraverso cartelli o adesivi ben visibili, di pubblicare sul proprio sito web, tre giorni prima dell'inizio delle riprese, le località visitate dalle vetture di Street View, stabilendo che per le grandi città è necessario indicare i quartieri in cui circolano le vetture. Analogo avviso doveva essere pubblicato da Google sulle pagine di cronaca locale di almeno due quotidiani e diffuso per mezzo di un'emittente radiofonica locale per ogni regione visitata.

Secondo il Garante Privacy, Google "ha effettuato illecitamente il trattamento di dati personali degli interessati in quanto ha reso loro una informativa che risulta non idonea". Si fa riferimento alle "peculiari caratteristiche delle fotografie scattate da Google Inc., che, oltre ad essere oggetto di diffusione online per un considerevole periodo di tempo, possono essere ingrandite per consentire all'utente una visualizzazione dettagliata delle stesse" nonché "le numerose segnalazioni pervenute all'Autorità, relative proprio all'acquisizione di immagini da parte della società che, nel fotografare i luoghi, ha ripreso anche soggetti identificabili che non desideravano comparire sulle fotografie pubblicate online da Google". Per determinare l'entità del danno, il Garante ha precisato che "la violazione è relativa a trattamenti che riguardano una considerevole quantità di dati personali di utenti e di altre persone acquisiti su porzioni rilevanti dell'intero territorio

nazionale, destinati alla successiva diffusione sul web". Inoltre, "l'elemento soggettivo della colpa relativo alla violazione in questione assume caratteri di maggiore gravità in relazione alla circostanza che ad un'azienda come Google, che fonda la propria attività economica prevalentemente sul trattamento dei dati e che costituisce uno dei principali fornitori mondiali di servizi della società dell'informazione, è richiesta la massima attenzione e diligenza negli adempimenti in tema di protezione dei dati personali, anche in funzione del potenziale rilevante impatto di eventuali violazioni". Per commisurare l'importo della sanzione alla capacità economica di Google, il Garante ha dovuto considerare i dati relativi al bilancio del 2012, in cui l'azienda ha registrato un fatturato consolidato di oltre 50 miliardi di dollari, con un corrispondente utile consolidato di 10,7 miliardi di dollari. Dopo qualche settimana Google ha pagato la sanzione di un milione di euro.

REDAZIONE

Obiettivo Europa - è l'inserto della newsletter di Consumers' Forum Dialogo Aperto, supplemento alla testata Help Consumatori.

Direttore Responsabile: Antonio Longo

Per Help consumatori: Antonella Giordano
Editore: Consumedia S.c.a.r.l. -Via dei Liburni 2 00185 Roma RM- P.IVA 08759041000
Reg. Trib. di Roma Sez. Stampa
n. 260/06 del 27 Giugno 2006

Responsabile Consumers' Forum: Alessandra Piloni
Web master: Giacomo D'Orazio
Grafica: Valentina D'Angelo