Oggetto: Consultazione pubblica sulla neutralità della rete

Martedì 4 maggio 2011

Illustre Presidente,
Illustri Commissari,

vorrei ringraziarVi, a nome dell'Istituto Italiano per la Privacy, per l'opportunità di contribuire alla consultazione qui in oggetto, è una straordinaria occasione per migliorare lo sviluppo di Internet e delle tecnologie e dei servizi ad essa collegati in Italia.

Come Istituto Italiano per la Privacy siamo contrari a qualsiasi nuova regolamentazione che miri ad imporre una rete "assolutamente neutrale", cioè un appiattimento generalizzato e indifferenziato delle reti senza alcuna gestione del traffico e con nessuna eccezione. In questo contributo sintetico Vi proponiamo quindi alcuni argomenti puntuali e specifici, che speriamo possano essere di Vostro interesse per una riflessione produttiva e che, soprattutto, possano rivelarsi di aiuto per giungere ad una decisione (il cui fine, ne siamo certi, sarà comunque l'interesse degli utenti bilanciato con le libertà di mercato e, di conseguenza, il miglioramento di Internet).

Rappresentando un Istituto di ricerca ed elaborazione di politiche a favore e tutela della privacy e della sicurezza dei dati personali, affronteremo il tema della rete neutrale, e delle ragioni per cui siamo fortemente contrari ad essa se non equilibrata e "dosata", unicamente dal punto di vista della tutela della vita privata e dei dati degli individui. Non risponderemo quindi a tutte le 10 domande da Voi elaborate ma, semplicemente, forniremo un commento che rispecchia la posizione dell'Istituto *ratione materiae*. Teniamo anche a sottolineare che, in qualità di centro studi che raccoglie al suo interno esperti e professionisti con competenze, interessi e orientamenti molto differenti, da cui deriva la nostra ricchezza, la posizione qui espressa rappresenta l'Istituto nel suo insieme, ma non ogni suo singolo Socio.

Perché una rete "troppo neutrale" lede la privacy e la protezione dei dati personali

La privacy degli individui si può proteggere in vari modi: uno è l'anonimato totale, che prevede una società (elettronica, in questo caso) del tutto imperscrutabile, sia nel bene sia nel male, dove ciascuno non sia riconoscibile né, di conseguenza, responsabile delle proprie azioni e parole; un secondo metodo, più evoluto ed equilibrato, consiste invece nella tutela dei dati e delle identità per gradi e principi che tengono conto di tre elementi fondamentali: la possibilità di scelta degli

individui, la sicurezza dei dati e delle infrastrutture che li ospitano/trasportano, la necessità di trasparenza e correttezza (anche on line) nel trattamento delle informazioni.

Gli articoli 7 e 8 della Carta dei diritti fondamentali della UE hanno sancito in maniera definitiva l'importanza della normativa privacy (intesa come protezione della vita privata, dell'identità e dei dati personali all'interno dell'Unione Europea). Inoltre, una serie di eventi ed evoluzioni hanno dimostrato che la tutela di questi diritti va intensificata a maggior ragione quando si parla di tecnologie dell'informazione e della comunicazione. Dalla crescita esplosiva di Facebook alla capacità di Google di raccogliere e indicizzare ogni tipo di informazione, abbiamo imparato che la privacy va aiutata e incentivata anziché trascurata: una questione centrale della rivoluzione digitale dei nostri tempi.

Quando si tratta di regolamentazione dell'infrastruttura di rete, la privacy viene spesso tristemente ignorata dai sostenitori della "neutralità totale": invece, mentre si cerca di definire un solido quadro normativo, primario e secondario, per la governance di Internet, le misure di protezione della privacy devono essere garantite ed in nessun modo limitate.

I fautori della rete "totalmente neutrale" avanzano la pretesa che questa posizione – tra le varie doti utopistiche ad essa riferite – garantisca l'impossibilità da parte degli Internet Service Providers (ISPs) di "monitorare" l'attività degli utenti e che quindi assicuri agli individui uno straordinario livello di privacy. Tutto ciò è sicuramente il riflesso di una profonda incomprensione della disciplina in materia di protezione dei dati nonché del ruolo degli ISPs e di come questi operino al fine di gestire al meglio il traffico della rete, la sicurezza dei suoi utenti e la loro privacy. Gli ISPs sono oggi in grado di gestire intelligentemente il traffico della rete attraverso appositi strumenti e pratiche di "traffic management" che tengono conto di criteri soggettivi (mittente, destinatario) e oggettivi (velocità, mole dei dati) in nessun modo invasivi rispetto alla privacy degli individui (altro e diverso, come impatto sulla vita privata, è l'utilizzo della cosiddetta "deep packet inspection" che "entra nel merito" della qualità dei dati, li analizza nel contenuto, per poi discriminarne il traffico: è questa una pratica da limitare a casi eccezionali e solo quando intervengano il consenso dell'utente o importanti ragioni di sicurezza o altri provvedimenti di rilievo pubblico). Il traffic management "neutrale" (cioè quello operato secondo criteri non invasivi) non riguarda il "monitoraggio" dell'attività dell'utente, ma consiste semplicemente nella gestione del traffico al fine di garantire un migliore servizio o, semplicemente, al fine di garantire il servizio sottoscritto dall'interessato, nella massima affidabilità e sicurezza delle infrastrutture. La gestione del traffico ha come fine ultimo l'utente e il servizio che ad esso viene fornito.

La pratica del "traffic management" permette anzi agli ISPs di operare al fine di assicurare la tutela della privacy degli utenti della rete, e la riduzione del rischio di perdite o disfunzioni nel trattamento dei loro dati. Per esempio, un fornitore di servizi di accesso alla rete ISP è in grado di offrire ai propri utenti, con il loro consenso, la possibilità di impedire o cancellare l'immagazzinamento dei loro dati da parte di terzi attraverso una serie di azioni quali, per esempio, il blocco selettivo di cookies o il rifiuto di richieste da parte di fornitori di contenuti e applicazioni. Questo servizio è un vantaggio per gli utenti e i consumatori in generale, per i quali Internet rappresenta un'incredibile opportunità ma comporta anche una serie di rischi da evitare, primo fra tutti quello della perdita di controllo sui propri dati. Dalle truffe online ai virus, fino a isolate pratiche predatorie di alcune applicazioni e contenuti forniti da imprese poco serie, la rete Internet ci presenta – esattamente come il mondo off line – una quantità di problemi e ostacoli che, se non affrontati, possono rappresentare un pericolo per i naviganti. Tali problemi possono essere affrontati e risolti attraverso un insieme di regole che, tuttavia, non soffochino e non sbilancino Internet a favore di posizioni ideologiche e parziali, seppure apparentemente nobili, oltre che grazie alla tecnologia stessa, che è in grado di sviluppare soluzioni (Privacy Enhancing Tecnologies) attente alla protezione dei dati e della riservatezza.

Ciò che conta, dal punto di vista del singolo interessato-utente, è conoscere esattamente quale gestione di rete venga eseguita, avere rispettati i propri diritti consumeristici (evitando clausole o pratiche abusive), essere informato compiutamente sulle modalità e finalità e sugli strumenti adottati per ogni attività che implichi il trattamento dei propri dati, avere piena possibilità di scelta in ordine al livello di servizio da richiedere all'ISP, anche con riferimento a possibili protezioni da "invasioni nella privacy" da parte dell'ISP o di terzi operatori on line.

C'è poi un secondo, rilevante aspetto del dibattito sulla neutralità della rete, un'altra "faccia della medaglia" che ha impatti sulla protezione delle informazioni nel senso della loro corretta "rappresentazione" (ricordiamo che la trasparenza dei trattamenti e l'esattezza, la completezza e l'aggiornamento dei dati in circolazione sono principi di grande valore in materia privacy): molto spesso, la richiesta di gestire il traffico intelligentemente è direttamente imputabile ai content providers/over the top o comunque a provider di servizi della società dell'informazione (VoIP, cloud computing, ecc.). Essi sono perfettamente consapevoli della limitata disponibilità di banda in precisi momenti e luoghi, per cui desiderano assicurare ai propri utenti una navigazione rapida, velocità di download e rapidità di accesso ai propri contenuti.
Ebbene, è evidente che in questo caso i pericoli sono di due tipi: quello concorrenziale tra operatori (e immaginiamo che l'Autorità stia lavorando intensamente su questo tema) e quello dell'impatto di eventuali esclusive di distribuzione di contenuti/servizi, frutto di accordo tra ISPs e altre imprese, sulla libertà di informazione dei cittadini-utenti.
Da tempo, come Istituto, puntiamo il dito verso certe discutibili pratiche di motori di ricerca e altri content providers, i quali si arrogano il diritto di decidere quali informazioni e quali dati personali siano accessibili per primi o in assoluto agli utenti, così, in ultima istanza, decidendo quale "cultura" e quale "informazione" e quali "identità" possano circolare sulla rete e quali, invece, ne siano escluse. Questo sarebbe un problema successivo e non direttamente correlato con la net-neutrality, se non intervenissero accordi di distribuzione privilegiata tra ISPs e content providers. Essendovi la possibilità di tali accordi, la questione diventa rilevante anche per gli equilibri infrastrutturali: per tale motivo, sosteniamo con forza l'idea che nessun accordo di distribuzione, pur lecito e che includa gestione del traffico, possa in alcun modo impedire la trasmissione, sebbene a velocità minori ma non eccessivamente penalizzate, di contenuti "liberi", provenienti cioè da content providers non "convenzionati" con l'ISP. In sostanza: anche in questo caso, sì al traffic management ma no alle assolutizzazioni, sia in un senso (neutralità) sia nell'altro (gestione della rete).

Il ruolo dell'Istituto Italiano per la Privacy è anche quello di facilitare l'integrazione tra l'operato del legislatore (con proposte pubbliche di riforma), gli esperti del settore privacy e sicurezza, e gli ingegneri sviluppatori di nuove tecnologie. Attraverso questa interazione è possibile favorire un migliore sviluppo della rete, un'evoluzione che possa garantire una più rapida crescita del mercato e una efficace tutela degli utenti.

Il Cloud Computing rappresenta il contesto ideale per dimostrare quanto qui sosteniamo. Il Cloud Computing pone una serie di problematiche cruciali per la protezione dei dati, proprio perché una delle sue funzioni principali permette agli utenti di elaborare, immagazzinare e trasmettere propri dati all'interno di un sistema gestito da una terza parte, cancellandone il controllo fisico. Chiaramente il Cloud può funzionare solo se l'infrastruttura su cui si sostiene è gestita in modo intelligente, cioè permettendo di fornire un servizio su misura che ne garantisca la totale affidabilità, sicurezza e protezione dei dati (protezione significa anche portabilità, accesso e controllo).

Per quanto concerne, invece, il fenomeno degli user-generated-contents, la gestione dell'infrastruttura consente di aggiungere un ulteriore livello di protezione della privacy, limitando e proteggendo l'accesso ai dati personali da parte di chi non ha diritto di accedervi. Una rete gestita

in modo intelligente, che non monitora gli utenti, consente a questi di navigare in modo autenticamente anonimo, ma protetto e responsabile delle proprie azioni: il singolo utente potrebbe scegliere di navigare attraverso una rete Internet sicura e protetta, decidendo se e quante informazioni personali condividere. Allo stesso tempo, la battaglia contro i crimini informatici sarebbe più efficace, perché ogni utente potrebbe essere smascherato dall'Autorità giudiziaria competente se operasse illegalmente. Anche qui risiede una minaccia alla protezione dei dati personali rappresentata dalla rete "totalmente neutrale" (e da qualsiasi tentativo più o meno originale di regolare la rete secondo modelli ideologici): privacy non significa "incognito" o "segreto" o "anarchico", significa gestione proporzionata e responsabile dei dati degli individui, per la tutela della loro libertà e della loro dignità.

La rete "totalmente neutrale" non facilita, infine, l'innovazione, al contrario la riduce come ogni forma di regolamentazione basata sulla limitazione, anziché sull'indirizzo e sull'incentivo di best practice, del progresso tecnologico. Se saranno forzati a sviluppare e mantenere reti statiche e poco intelligenti, ottuse, gli operatori non saranno stimolati a produrre valore aggiunto e quindi ad investire. Le conseguenze sono tanto prevedibili quanto dovrebbero orientarci ad evitare di perseguire un obiettivo così sbagliato: i sostenitori della rete "totalmente neutrale" non considerano nessuna delle conseguenze negative che deriverebbero dall'implementazione di lacci e norme in grado di appiattire ogni distinzione tra utenti, tra imprese. Quel che oggi può apparire loro come una buona legislazione potrebbe risultare, invece, un ostacolo alla protezione dei consumatori in futuro. In altre parole, il tentativo di rendere tutti i soggetti della rete uguali (non lo sono, perché hanno esigenze differenti) si abbatterebbe come un boomerang sugli utenti stessi, presentando loro un servizio proiettato al regresso radicale e alla mancanza di sicurezza e affidabilità di Internet.

Mentre noi accogliamo positivamente questa discussione perché siamo convinti che aiuti ad affrontare i problemi con strumenti migliori, trovando soluzioni efficaci ed economiche, ci permettiamo di suggerire a questa Autorità di evitare di intraprendere azioni troppo affrettate su questo tema. Il dibattito sul concetto di rete neutrale ha evidenziato posizioni spesso estreme e in totale contrasto tra loro; il concetto di rete neutrale è molto complesso, anche perché coinvolge aspetti tecnici e giuridici che spesso sfuggono ai più e che sono in costante evoluzione: ottima è la misura.