Roma, e-privacy Giovedi 2 luglio 2015

Camera dei deputati

Sala dei gruppi parlamentari

La sicurezza come diritto di libertà e il ruolo della privacy nel prossimo futuro

di Stefano Aterno

La sicurezza non più concepita in contrapposizione con la privacy e con la libertà quasi che la richiesta dell'una necessariamente comporti una conseguente diminuzione o attenuazione dell'altra.

La sicurezza come una delle molteplici espressioni del diritto di libertà, uno dei tanti, che come la riservatezza e al pari di essa sia consacrato esplicitamente e implicitamente nella nostra Costituzione. Una sicurezza quindi conseguentemente democratica che contiene in sè, come la privacy i valori ed i limiti propri di ciascun diritto di libertà. Nuovi concetti della sicurezza non più concepita in contrapposizione con la privacy e con la libertà quasi che la richiesta dell'una necessariamente comporti una conseguente diminuzione o attenuazione dell'altra.

Concetti di sicurezza e privacy adeguati ai tempi e strettamente legati tra loro in quell'indissolubile legame che deve esistere tra diritti sociali e diritti di libertà. Il ruolo della privacy e della sua legislazione assume in questo ambito un ruolo di garanzia e di controllo in funzione di quel giudizio di responsabilità che deve esistere affinché quest'apparente dicotomia si mantenga sempre nel giusto equilibrio.

*Questo intervento nasce da alcune riflessioni degli ultimi mesi e da alcuni appunti presi con il tempo durante i mie studi in tema di privacy, di sicurezza e di indagini forensi. Appunti nati anche da alcune norme introdotte nel nostro ordinamento dalla recente legge antiterrorismo come le modifiche sulla data retention e sull’acquisizione dei dati informatici all’estero senza rogatoria con il consenso del titolare del servizio on line ex art. 234 bis del codice di procedura penale.*

Lo spionaggio, la sorveglianza e la conseguente aggressione alla privacy dei cittadini e di interi stati sovrani fa sempre più spesso notizia. Il concetto di sicurezza e di sorveglianza è da decenni in totale espansione, è diventata una caratteristica costante e fondamentale del mondo moderno. Un mondo moderno che per dirla come Bauman è un mondo liquido. Si parla di modernità liquida come nuovo genere di modernità intendendola come individualizzata, privatizzata, incerta, flessibile, vulnerabile. Cittadini, lavoratori, consumatori, navigatori della Rete sono sempre in movimento spesso privi di certezze ma accettano il rischio che i loro movimenti vengano monitorati, tracciati, localizzati e profilati. Anche l’esigenza di sicurezza e la necessità di privacy scivolano poco a poco in uno stato fluido. L’esigenza di sicurezza e quindi la capacità di sorveglianza sui dati personali dilaga ovunque. Un tempo la sorveglianza era solida, stabile in qualche modo

garantita da principi giuridici certi e da punti di riferimento indiscutibili. Oggi la sorveglianza tende a farsi liquida soprattutto nei momenti in cui frammenti di dati personali, trattati per determinate finalità, divengono facilmente utilizzabili per altri scopi.

Prima di affrontare il tema centrale del problema che qui si vuole porre alla vostra attenzione occorre premettere che ormai quando parliamo di privacy dei nostri dati abbiamo di fronte un “doppio binario”: da un lato il trattamento dei dati dei consumatori, la profilazione delle nostre abitudini a fini di marketing e di studio del comportamento umano e dall’altro il trattamento dei dati per accertamento e repressione dei reati e per esigenze di sicurezza nazionale. In quest’ultimo ambito molte sono le deroghe ai principi generali.

Riguardo alla prima tipologia di trattamento e al suo rapporto con il diritto alla riservatezza è ormai chiaro a tutti che la privacy non gode di ottima salute……

Senza cercare altrove fantomatici colpevoli è sufficiente che ciascuno di noi si guardi allo specchio: siamo noi per nostra volontà a mandare al massacro il nostro diritto alla privacy. Nella migliore delle ipotesi, spesso con una colpa che definirei “una colpa cosciente” acconsentiamo a perdere la privacy perché lo consideriamo un costo ragionevole da pagare in cambio dei meravigliosi servizi che ci vengono offerti. Ci rifiutiamo di leggere le condizioni di contratto dei servizi e le informative su “app” e software che scarichiamo con lo stesso atteggiamento colpevole di cui sopra. Al limite tra la colpa cosciente e il dolo eventuale stiamo uccidendo la nostra privacy. Moltissimi adolescenti in relazione ad “app” e social network usano il proprio smartphone come un “confessionale elettronico portatile” e forse ..non solo gli adolescenti..…

All’apparenza, spesso ci viene offerto uno straccio di contratto bilaterale che almeno formalmente, il più delle volte in uno stato straniero, ci riconosce il diritto di sporgere reclamo o fare causa. A questo proposito, per rappresentarvi in senso figurato ciò che sta a mio avviso accadendo e il grado di percezione del rischio vi racconto il famoso esperimento della rana bollita che risale ad una ricerca condotta dal John Hopkins

University nel lontano 1882 (un amico me lo raccontò tempo fa e so che viene utilizzato anche per illustrare scenari socioeconomici): *se prendiamo una rana e la mettiamo dentro una pentola con acqua bollente la rana salta e scappa via perché si accorge che l’acqua brucia. Se invece prendiamo la rana e la mettiamo nella pentola e solo dopo accendiamo lentamente ma in modo costante il fuoco la rana finisce inevitabilmente bollita senza accorgersene, se non troppo tardi…*

E’ esattamente ciò che sta accadendo nel nostro rapporto tra l’utilizzo delle nuove tecnologie e la nostra privacy…..è bollita…

Per uscire da questa sorta di prigione, nella quale ci siamo infilati forse anche inconsapevolmente, possiamo confidare nelle leggi, nelle direttive e nei regolamenti europei ? La risposta potrebbe essere in parte positiva almeno per la prima tipologia di trattamento (marketing e privacy). Almeno sotto alcuni punti di vista un certo grado di protezione esiste e si riesce a garantire anche se il L(l)egislatore (spesso scritto con lettera minuscola) fatica a scrivere norme frutto di ragionamenti ponderati e condivisi ed è troppo spesso preso dalla fretta e dalla disattenzione. Il Regolamento Europeo sulla privacy, ormai da anni in elaborazione presso gli organismi europei è stato oggetto dell’ assalto di decine e decine di emendamenti che lo stanno erodendo nei contenuti snaturandolo rispetto al testo iniziale e quindi a quelle che erano le intenzioni iniziali. I paesi membri dell’Unione Europe quando lo presentarono, tra il 2012 e il 2014, avevano accantonato la paura del terrorismo e l’esigenza di conservare un certo grado di sicurezza interna che invece oggi hanno dovuto recuperare a causa dei gravi episodi recentemente accaduti. Di fatto sta accadendo che molte delle questioni che erano oggetto del Regolamento sono state separate e confluiranno in due diverse direttive europee che dovranno essere recepite con apposite norme interne da ciascuno degli stati membri che cosi facendo eserciteranno una loro propria discrezionalità distaccandosi dai principi ispiratori di un tempo.

Ciò posto, seppur con difficoltà e con molto egoismo da parte degli stati membri (sempre ancora più stati membri piuttosto che Stati Europei), prima o poi il Regolamento europeo verrà approvato definitivamente. Con tale approvazione, bene o male, al di là dei principi e di molte norme già oggi presenti nel codice vigente, si

disciplinerà tutto il rapporto tra la privacy dei consumatori e il trattamento dei dati da parte dei titolari dei servizi on line. Particolare attenzione verrà attribuita al trasferimento dei dati all’estero e al trattamento attraverso i servizi di cloud computing. Certo, rimane da chiedersi se dopo tanti anni dalla sua iniziale stesura questo regolamento non nasca già vecchio….. ma tant’è !…..Non ci resta che affidarci al legislatore europeo (con la l minuscola) sperando in un momento di illuminazione ……anche solo occasionale.

**La seconda tipologia di trattamento** è quella tipica del trattamento dei dati (personali e non) per accertamento e repressione dei reati e per esigenze di sicurezza nazionale.

In questo ambito i continui e repentini cambi di fronte tra periodi di grandi richiami alla “privacy nel mondo” e periodi tipici di uno stato dell’emergenza o per dirla come Agamben “uno stato d’eccezione” il rischio di rovinare anche quel livello minimo di garanzie è molto alto. Ma è anche molto alto il rischio di non avere alcuna sicurezza.

NON è possibile continuare a barcollare tra improvvisi momenti tipici di uno stato dell’emergenza e repentini cambi di rotta in senso “privacy- integralista”. Non è possibile continuare a navigare a vista tra rischi veri o presunti di violazione della privacy, abusi reali della riservatezza dei cittadini ed esigenze concrete di sicurezza nazionale, sicurezza informatica e di accertamento e repressione dei reati che creano da un lato un drastico affievolimento del diritto alla privacy senza soddisfare dall’altro lato l’esigenza di un reale potenziamento della lotta alla criminalità e al terrorismo.

Il risultato negativo e palpabile è sotto gli occhi di molti. I cittadini non godono né di un diritto pieno alla privacy né concepiscono la sicurezza come diritto fondamentale. Il rischio è che l’aggiunta di una schizofrenia anche legislativa e politica contribuisca a creare confusione di valori e integralismi da ambo i lati; in funzione del periodo e delle circostanze. L’assenza di principi fondamentali e di equilibrio che contemperino situazioni apparentemente dicotomiche ma in realtà sinergiche, rischia di creare fenomeni di integralismo temporaneo che minano proprio la ricerca del punto di equilibrio, la giusta lettura e interpretazione dei problemi; un punto in cui la sicurezza e la privacy devono necessariamente finire per bilanciarsi sostenendosi a vicenda.

E’ impossibile ! …..potrebbe dire qualcuno ma forse si sbaglia.

La sicurezza deve essere oggi concepita e sentita come una delle molteplici espressioni del diritto di libertà uno dei tanti diritti di libertà, come la riservatezza e al pari di essa consacrati esplicitamente e implicitamente nella nostra Costituzione. Una sicurezza quindi conseguentemente democratica che contiene in sè, come la privacy i valori ed i limiti propri di ciascun diritto di libertà. E’ concettualmente errato e superato, pensare alla sicurezza come prerogativa del potere costituito e le libertà come diritto del popolo e del cittadino di sottrarsi ad esso.

E’ invece proprio questa vecchia teoria della sicurezza che in maniera esplicita o implicita teorizzava politiche di repressione e prevenzione di polizia tendenti spesso a garantire l’ordine e a comprimere alcune libertà.

Occorre pensare diversamente, occorre pensare che se è imprescindibile in uno stato moderno affermare, in modo fermo e convinto, il diritto alla sicurezza, lo è altrettanto, difendere il principio della sicurezza di ogni diritto di libertà e quindi anche del diritto alla riservatezza dei dati personali. L’equilibrio tra il diritto alla sicurezza e la sicurezza del diritto alla privacy, per dirla con le parole del prof. Carlo Mosca, mio Maestro, colgono con efficacia i parametri di un ragionamento che ritroviamo nei canoni costituzionali e che intende fornire OGGI una lettura nuova e garantista dei profili delicati di una questione altrimenti destinata ad impostazioni vecchie e di stampo autoritario.

Interpretazioni orientate all’equilibrio senza ricorrere continuamente a deroghe di regole fondamentali (esempi recenti in materia di rogatorie internazionali o in tema di intercettazioni informatiche) evitano il rischio di fratture costituzionali di cui non si è in grado di valutare conseguenze.

L’ alto livello di sicurezza (con compressione e affievolimento della riservatezza dei cittadini) e il rispetto della privacy degli stessi possono coesistere, possono operare in sinergia e tenersi in equilibrio se alla base vi è un costante richiamo al senso e al dovere

di RESPOSABILITA’. Se è vero come è vero che Libertà è innanzitutto Responsabilità (art. 2 Cost.) il richiamo a quest’ultima deve essere molto più forte e presente nella normativa di settore di quanto non lo sia ora. Ma soprattutto deve essere un punto fermo culturale.

La responsabilità giuridica che investe chi tratta i dati personali non copre in modo omogeneo tutti i tipi e gli ambiti di trattamento. Il criterio cardine di cui all’art. 2050 del codice civile che regola il trattamento dei dati personali ex art. 11 e 15 del codice privacy non si applica in certi ambiti anche molto delicati.

Sono tanti anni ormai che personalmente mi confronto ogni giorno con le norme in tema di privacy, con i provvedimenti dell’Autorità Garante, con la trasparenza, con il processo penale e mi domando se tutta questa legislazione materia non sia forse eccessiva, ridondante e forse caricata di adempimenti e troppi passaggi “burocratici”. Ecco, alla base, forse occorreva una spinta culturale ed educativa più decisa. E’ diventata imprescindibile una nuova e più profonda cultura della privacy che miri a permeare non solo gli addetti ai lavori, ma ogni individuo, ogni titolare del trattamento dei dati. Occorre una sensibilità nuova del rispetto della privacy e della riservatezza.

L’equilibrio tra un diritto alla sicurezza (costante e completo) e una sicurezza del diritto di libertà potrebbe essere sostenibile e garantito proprio da una maggiore accountability e da un maggiore senso di Responsabilità, di Etica e di Rispetto delle Istituzioni e delle Costituzioni da parte di tutti.

Grazie.

Stefano Aterno stefano@aterno.it