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

di Stefano Aterno

Negli ultimi tempi, fatti e circostanze mi hanno indotto a formulare alcune riflessioni sul tema della privacy, della sicurezza e sulle moderne tecniche delle indagini informatiche. Alcune norme su queste materie sono state introdotte nel nostro ordinamento dalla recente legge antiterrorismo e altre verranno votate dal Parlamento.
Nell'aprile del 2015 hanno visto la luce importanti modifiche sulla data retention e sull'acquisizione dei dati informatici all'estero senza rogatoria (art. 234 bis c.p.p.).
Quanto qui si dirà è in gran parte frutto dell'intervento tenuto in occasione del convegno di e-privacy 2015 alla Camera dei deputati – sala dei gruppi parlamentari il 2 luglio 2015 e quindi pochi giorni prima del caso Hacking team e qualche mese prima delle stragi di Parigi del novembre scorso.

La sicurezza non può più essere 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 deve essere intesa 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 quindi. 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.

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 sono da decenni in totale evoluzione. La sicurezza, 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 l'aumento della capacità di sorveglianza sui dati personali dilaga. 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 problema centrale che voglio porre alla vostra attenzione occorre premettere che ormai quando parliamo di privacy dei nostri dati abbiamo di fronte un concetto di riservatezza che si muove su 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 e la conservazione dei dati per finalità di accertamento, prevenzione e repressione dei reati nonché 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 da tempo 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 nostra privacy perché lo consideriamo un costo ragionevole da pagare in cambio dei meravigliosi servizi che ci vengono offerti. Con lo stesso atteggiamento colpevole rifiutiamo di leggere le condizioni di contratto dei servizi e le informative su "app" e software che scarichiamo sui nostri palamari o personal computer. 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 una sorta di "confessionale elettronico portatile" e forse ..non solo gli adolescenti..…

Ci viene offerto all'apparenza, 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 presso le corti di un lontano paese. 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…….la nostra riservatezza 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 fatica a scrivere norme frutto di ragionamenti ponderati e condivisi ed è troppo spesso preso dalla fretta e poco attento ai cambiamenti di lungo periodo. Il Regolamento Europeo sulla privacy, ormai da anni in elaborazione presso gli organismi europei è stato finalmente definito e nei prossimi giorni, dopo la traduzione, verrà emanato dall'Unione Europea per entrare in vigore in tutti i Paesi membri 24 mesi dopo.
Il regolamento però negli anni è stato oggetto di continui interventi ed emendamenti che lo hanno, in parte, eroso nei contenuti snaturandolo rispetto al testo iniziale e alle intenzioni dei primi estensori. Quando fu presentato, tra il 2012 e il 2014, l'Europa aveva accantonato la paura del terrorismo e l'esigenza di avere un alto livello di sicurezza interna; oggi, a causa dei gravi episodi recentemente accaduti la paura e la sicurezza tornano a dettare l'agenda politica e si assiste basiti al tentativo in alcuni Stati di sospendere l'ordine giuridico o comunque a limitarlo fortemente nei settori delle libertà e dei diritti fondamentali.
Si sta assistendo al ritorno dello "stato di eccezionalità" seppur in taluni ambiti.
Da almeno un anno molte delle questioni che erano oggetto del Regolamento sono state separate e inserite in due diverse direttive europee (una per esempio in tema di trattamento dei dati giudiziari e per finalità di indagini penali) che verranno recepite da ciascuno degli stati membri che, in quell' ambito specifico, potranno esercitare una loro propria discrezionalità distaccandosi dalle norme richiamate nel Regolamento.

Ciò posto, seppur con difficoltà e con molto egoismo da parte degli stati membri (sempre ancora più "stati membri" e sempre meno Stati Europei), il Regolamento europeo è stato approvato definitivamente. Con tale approvazione, bene o male, al di là dei principi e di molte norme già oggi presenti nel codice vigente, si è disciplinato 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 (manca tutta una parte relativa "all'internet delle cose"….. ma accontentiamoci.

La seconda tipologia di trattamento è quella tipica del trattamento dei dati (personali e non) per accertamento, prevenzione e repressione dei reati nonchè per esigenze di sicurezza nazionale.
In questo ambito, negli ultimi 15 anni abbiamo avuto 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 presenti è molto alto.
Ma è molto alto anche il rischio di non avere alcuna sicurezza reale.
NON è possibile continuare a barcollare tra tipici momenti 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, reali abusi della riservatezza dei cittadini ed esigenze concrete di sicurezza nazionale.

Da un lato, è certamente necessario aumentare la sicurezza informatica delle infrastrutture critiche del nostro paese ma attenzione a determinare 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 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' la vecchia teoria della sicurezza che in maniera esplicita o implicita teorizzava politiche di repressione 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, richiamando i concetti espressi dal prof. Carlo Mosca in un suo recente libro, 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, interventi illuminati del legislatore, senza ricorrere continuamente a deroghe di regole fondamentali (esempi recenti in materia di rogatorie internazionali o in tema di intercettazioni informatiche anche mediante Trojan "di Stato") 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 RESPONSABILITA'. 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 dei trattamenti. 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. E' un tema questo che in epoca di corsa a norme "eccezionali" deve essere tenuto presente.

A proposito di norme eccezionali, consentitemi due parole sul cd Trojan di Stato o captatore informatico a cui prima facevo riferimento. Dal 2004 al 2012 (più o meno) è stato utilizzato da magistratura e forze dell'ordine con la "copertura giuridica" sbagliata e ridicola della "prova atipica" (ex art. 189 c.p.p) come, disgraziatamente, una sentenza della corte di cassazione del 2009 aveva stabilito.
Poi, in quest'ultimi anni, è stato utilizzato, sempre per reati gravi e reati informatici, ricorrendo alla "quasi" più solida copertura dell'art. 266 bis c.p.p. e delle norme sull'intercettazione ambientale audio- video. In queste ultime ipotesi, salvo errori giuridici e tecnici di PM, GIP e forze di polizia (si veda la sentenza di annullamento della Cassazione del giugno 2015 sull'intercettazione ambientale sul telefono cellulare), siamo all'interno del codice di procedura penale.
Ma appare evidente che non è assolutamente sufficiente né soddisfacente la soluzione di ricondurre tutto sotto l'art. 266 bis c.p.p.
Chi conosce il funzionamento dello strumento[1] sa bene che lo stesso fa molto di più che captare audio, video e flussi di dati che entrano in un PC o in un cellulare. Egli sa anche che lo strumento non capta solo il flusso ma prende i dati memorizzati sul sistema (che non sono mai stati oggetto di flusso o che lo sono stati prima dell'attivazione dell'intercettazione). La seconda ipotesi non è proprio intercettazione informatica…
L'uomo avveduto sa che il software può prendere anche dati giacenti nel sistema e non solo quelli frutto di flussi informatici. Un esempio ? una foto scattata con il cellulare e mai spedita o condivisa con nessuno….
È una remote forensics vera e propria. Ovviamente occulta e irripetibile. Vogliamo continuare a far finta di nulla ? Vogliamo provare a scrivere negli atti di indagine cosa il captatore deve prendere e cosa NON deve prendere ?
Vogliamo cominciare a scrivere negli atti processuali di indagine che è stato usato il captatore informatico invece di scrivere genericamente che si è trattato di intercettazioni

[1] Chi lo utilizza o autorizza l'uso deve sapere esattamente tutto ciò che fa e che può fare il software alla base del sistema di captazione e soprattutto deve controllare o delimitare i poteri di colui che lo utilizza in concreto soprattutto se quest'ultimo non è un agente o un ufficiale di polizia giudiziaria.

informatiche ? I decreti generici di intercettazione telematica non bastano. Non si tratta solo di intercettazioni telematiche e le diverse attività non sono separabili, eliminabili né scomponibili a piacimento dai magistrati e da chi capta in concreto.
Vogliamo cominciare a sederci ad un tavolo e parlare di come legiferare l'utilizzo dello strumento ? Vogliamo considerare le diverse soluzioni normative che qualcuno sta scrivendo nelle stanze del Parlamento ?
Vogliamo affrontare il delicato problema dell'inutilizzabilità (o meno) di certe captazioni da remoto ?
Oppure dobbiamo attendere il solito e maledetto decreto legge frutto dell'emergenza, dell'eccezionalità del momento, che butterà la "privacy" con tutta l'acqua sporca !

Sono tanti anni ormai che personalmente mi confronto ogni giorno con la complessità delle norme in tema di privacy, con i provvedimenti dell'Autorità Garante, con i problemi dell'informatica nell' ambiente di lavoro, con il processo penale e le investigazioni private e fin tanto che mi occupo di questo come avvocato o come consulente posso anche valutare, egoisticamente, gli effetti positivi di tale complessità e, a volte, di tale confusione.
Però, da cittadino che osserva il comportamento delle persone e delle aziende alle prese quotidianamente con il problema "privacy" mi domando se questi "soggetti" non siano piuttosto sull'orlo di una crisi di nervi, e se non siano utili piuttosto continui interventi con linee guida interpretative e chiarificatrici.

Ecco, alla base e prima di ogni tentativo europeo di regolamentare la vastissima materia, forse occorreva (procedendo in qualche forma anche in parallelo) investire tempo e risorse per fornire in modo più chiaro una maggiore spinta culturale ed educativa.
Oggi, alle porte del 2016, è diventata imprescindibile una nuova e più profonda cultura della privacy finalizzata a permeare non solo gli addetti ai lavori, ma ogni individuo, ogni titolare del trattamento dei dati.
E' necessario che ciò avvenga proprio oggi, in un momento in cui l'esigenza di sicurezza sta affievolendo alcuni tra i diritti fondamentali.
Occorre una sensibilità nuova del rispetto della privacy e della riservatezza.
L'equilibrio tra un diritto alla sicurezza e una sicurezza del diritto di libertà può essere sostenibile e può essere garantito dalla presenza, anche culturale, di maggiore accountability in tutta la materia.

Stefano Aterno
stefano@aterno.it

(lo scritto è frutto dell'aggiornamento di vecchi appunti e del discorso trascritto in occasione del convegno "E-privacy" del 2 luglio 2015 presso l'aula dei gruppi parlamentari della Camera dei Deputati).