Dr. iur. Michele Albertini
Residenza governativa
Via Canonico Ghiringhelli 1
6501 Bellinzona
segretariato 091 814 45 02
fax 091 814 45 09
E-Mail protezionedati@ti.ch
Web www.ti.ch/protezionedati

Cittadino e privacy

Internet tra diritti e obblighi d'informazione

Traccia della relazione tenuta il 23 ottobre 2003 nell'ambito del Convegno "Internet e sicurezza informatica: rischi e contromisure", Ticino Informatica 2003, Lugano

È determinante esclusivamente il testo esposto e sviluppato oralmente

Sommario

1. Introduzione: la privacy nella società dell'informazione
2. Internet e protezione dei dati
   2.1. L'autodeterminazione informativa e la sua concretizzazione
   2.2. Elaborazione e trasmissione di dati in forma telematica
   2.3. Internet e principi fondamentali della protezione dei dati
   2.4. Diritti e obblighi d'informazione oggi
   2.5. Diritti e obblighi d'informazione domani
3. Conclusione: autodisciplina, trasparenza e informazione quali premesse della privacy

1. Introduzione: la privacy nella società dell'informazione

Signore e signori,

quando mi è stato proposto di intervenire in questo importante dibattito - a cura del Clusis, del Clusit e di Ticino informatica, con la collaborazione della Polizia cantonale, a cui rivolgo il mio sentito ringraziamento - mi sono subito chiesto quale contenuto avrei potuto dare al mio esposto. Parlare di privacy nel contesto della libera accessibilità e del libero scambio di informazioni nella rete globale mi è infatti sembrato subito un tema complesso.

La prima difficoltà sta già nel capire se per il cittadino questo termine abbia ancora senso quando si pensi al grande uso che fa di internet, di posta elettronica, di carte di credito, di carte clienti, quando è l'interessato medesimo a fornire volontariamente i suoi dati – allettato forse da premi o da altri tipi di vantaggi – quindi a consentire ad altri, di fatto, di gestire i propri dati personali in ogni settore dell'odierna società dell'informazione.

Chissà se abbia ancora senso parlare di *"ambito gelosamente circoscritto della vita personale e privata"* - come si legge nel DEVOTO/OLI sotto la voce privacy - quando ogni giorno si guardano, si sentono, si leggono notizie sul cosiddetto "cliente trasparente" o, più in generale, sui grossi rischi per la riservatezza legati all'uso degli strumenti telematici, ma si continua a far capo indiscriminatamente alle loro prestazioni.

Una cosa è certa: con la formidabile esplosione della comunicazione telematica – e in particolare di internet e della posta elettronica – è aumentata la libertà del singolo di *dare e ricevere informazioni*, ma non in modo corrispondente quella di *opporsi* a questi flussi di informazioni**,** perlomeno se lo riguardano personalmente, o quella di *impedire* che terzi non autorizzati possano accedere a questi dati. Neppure, di fatto, è completamente garantita la libertà del cittadino *di essere informato* con precisione sui flussi di dati che lo riguardino.

Un'altra cosa è certa. Il concetto di privacy nella società dell'informazione assume contorni diversi da quelli a cui eravamo abituati in precedenza. Addirittura, proprio l'avvento di internet ha accentuato le connotazioni *altamente soggettive* del senso di riservatezza. La privacy è un momento intimamente legato alla personalità di ognuno. E ognuno la percepisce, la recepisce e la manifesta nel modo che più gli è congeniale. Qualcuno può arrabbiarsi alla notizia che una società commerciale conosca o valuti le sue abitudini consumistiche in base ai suoi acquisti, qualcun altro invece può approvare questo metodo, convinto che le offerte che gli provengono in modo mirato gli fanno risparmiare tempo nella scelta dei prodotti.

Ma sarebbe profondamente sbagliato, per questa ragione, diminuire le cautele e accontentarsi dell'autoregolamentazione del sistema. Non è certamente soddisfacente limitarsi ad indicare che colui che fornisce i propri dati o li inserisce egli medesimo in internet deve assumersi anche il rischio che terzi li elaborino in modo illecito o senza autorizzazione.

Si tratta invece di definire quali *misure minime* devono essere ritenute necessarie, a livello legislativo, per permettere a chiunque di poter esigere il rispetto della propria *"libertà di privacy"* e di poter navigare con più sicurezza nell'attuale società dell'informazione.

In questo contesto la *sicurezza informatica e la sicurezza dei dati* rivestono un ruolo senza dubbio determinante ed è giusto che la legge le esiga. Ma la sicurezza è un concetto molto ampio, non solo tecnico. Nella mia relazione vorrei attirare la vostra attenzione proprio su questo aspetto, mettendo a fuoco un elemento che sta alla base di qualsiasi misura tecnica di sicurezza: l'*informazione come strumento di prevenzione*. Con riferimento particolare ad internet, vedremo in che misura *diritti ed obblighi d'informazione* possono contribuire a migliorare il senso di privacy del cittadino.

Per focalizzare l'argomento mi pare doveroso illustrare il quadro normativo in cui ci muoviamo, ben cosciente che si tratta di un tema senza dubbio complesso e magari difficilmente comprensibile, poiché diversi temi, come vedremo, si intrecciano, e paiono a prima vista - ma solo a prima vista - fors'anche ripetitivi.

2. Internet e protezione dei dati

2.1. L'autodeterminazione informativa e la sua concretizzazione

Il testo della nuova Costituzione federale stabilisce che *"ognuno ha diritto d'essere protetto da un impiego abusivo dei suoi dati personali"*.

Questa norma non è invero molto soddisfacente nel suo tenore letterale, poiché la protezione dei dati non significa unicamente protezione da un impiego abusivo ma qualcosa di più profondo, come indica invece - in una formulazione sicuramente riuscita - la Costituzione cantonale, che garantisce esplicitamente la *"tutela della sfera privata e dei dati personali e il diritto di ciascuno di consultare ogni raccolta di dati ufficiali o privati che lo concernono, domandarne la rettifica se errati e esigere di essere protetto contro una loro utilizzazione abusiva"*. In realtà le norme richiamate sono univoche nel loro contenuto: già nel 1987 il Tribunale federale aveva riconosciuto il diritto fondamentale non scritto del cittadino di poter gestire in modo autonomo i dati che lo riguardano. Questo precetto - valido tuttora e componente essenziale della garanzia costituzionale - è anche chiamato *diritto all'autodeterminazione informativa* (meglio noto nella

diritto all'autodeterminazione informativa (meglio noto nella terminologia in lingua tedesca come "*Recht auf informationnelle Selbstbestimmung*"). Questo diritto significa in pratica che il cittadino deve poter decidere liberamente se rendere accessibili a terzi i suoi dati personali e come essi devono essere utilizzati. Deve anche poter decidere liberamente sulle forme e sui modi di gestione delle informazioni che lo concernono.

Com'è concretizzata questa garanzia? Anzitutto con le leggi generali sulla protezione dei dati. Ne abbiamo molte in Svizzera. Abbiamo quella federale del 19 giugno 1992, determinante per le elaborazioni di dati personali da parte di persone private e di organi pubblici federali, e abbiamo le legislazioni cantonali e - dove esistono - quelle comunali. Alla legge ticinese sulla protezione dei dati personali del 9 marzo 1987 sottostanno il Cantone, i Comuni, le altre corporazioni e istituti di diritto pubblico e i loro organi. A questi sono parificate le persone fisiche e giuridiche di diritto privato, cui siano demandati compiti pubblici.

In sostanza: il sistema svizzero prevede sempre - ed esaustivamente - l'applicabilità di una legge, fondandosi *su chi* elabora i dati. Quindi: per i rapporti tra privati è determinante la legge federale, per i rapporti tra organi pubblici federali e privati è applicabile ancora la legge federale, mentre per i rapporti tra organi cantonali (o comunali) e privati sono determinanti le leggi cantonali.

Tutte queste leggi hanno tratti essenziali che le accomunano: tutte perseguono lo scopo di proteggere i diritti fondamentali - in particolare la personalità e la sfera privata – delle persone fisiche e giuridiche. *In realtà è quindi la personalità ad essere tutelata, non i dati personali in quanto tali*.

In sostanza, la protezione dei dati di natura privata e quella pubblica seguono motivazioni analoghe, sia per quanto riguarda i principi generali sia per quanto concerne gli strumenti legali di protezione e di informazione.

Prima di approfondirli è utile chiarire alcuni concetti che mi sembrano importanti quando si pensi alla valenza della privacy del cittadino nel contesto di internet.

2.2. Elaborazione e trasmissione di dati in forma telematica

La nozione di *elaborazione o di trattamento di dati personali* è molto ampia: difatti con questo termine si intende ogni operazione intesa segnatamente (l'elenco non è esaustivo) a raccogliere, conservare, utilizzare, modificare, trasmettere o distruggere questi dati. E questo indipendentemente dagli scopi, dai modi e dalle procedure utilizzati. La nozioni nei diritti cantonali e nel diritto federale sono pressoché equivalenti.

Tra le componenti dell'elaborazione figura anche la *trasmissione o comunicazione di dati personali* (anche questo è un termine molto ampio) che si riassume nel fatto di rendere accessibili i dati a una cerchia determinata o indeterminata di persone, non necessariamente sottoposte a vincoli di segreto. Sono trasmissioni di dati ad esempio la divulgazione, la pubblicazione (quindi la diffusione a molte persone), oppure anche la semplice consultazione di dati personali.

Nell'ambito di internet queste definizioni sono importanti per *due ragioni sostanziali*. Da un lato perché consentono di includervi una moltitudine di azioni (per esempio è ampiamente riconosciuto che l'invio di un'e-mail e la messa a disposizione in internet di un documento contenente dati personali equivalgono a elaborazioni, e meglio trasmissioni o comunicazioni, di dati), dall'altro perché chi elabora i dati (le autorità e anche le persone private) è tenuto ad osservare precisi vincoli legali a tutela della privacy degli utenti.

2.3. Internet e principi fondamentali della protezione dei dati

Ma quali sono questi vincoli? In definitiva, l'elaborazione (compresa la raccolta di dati) deve essere effettuata in modo *lecito e leale*, e poco importa se avviene manualmente o in forma automatizzata. È lecita e leale quando è conforme alla legge, è sicura, trasparente, razionale ed è controllata e controllabile. Tutti questi elementi – ma potremmo aggiungerne altri – sono *interdipendenti*. Un'elaborazione di dati personali che non fosse trasparente non sarebbe neppure controllabile, e neppure sicura, e neppure conforme alla legge.

Dire se un'elaborazione di dati sia lecita o illecita, nell'accezione più ampia, è il risultato di un'analisi essenzialmente giuridica, che si fonda su queste domande:

- Chi può elaborare quali dati e per quale scopo?
- Dove e come possono essere raccolti ed elaborati i dati?
- A chi possono essere comunicati i dati?
- E infine ma non per ultimo: la persona interessata è a conoscenza dell'elaborazione?

Le risposte concrete – e sottolineo concrete - non si trovano nelle leggi sulla protezione dei dati, perché contengono solo *disposizioni quadro* e principi generali, principi guida di valenza universale. Il significato di questi *principi generali* e degli *scopi della protezione dei dati* è importante, perché essi vanno considerati nell'applicazione di qualsiasi norma che disciplini l'ambito dei dati personali. Le risposte concrete alle domande precedenti vanno ricercate nel diritto speciale o settoriale, che può prevedere soluzioni differenziate, creando così eccezioni o affinamenti giustificati dal tema specifico. Per esempio alcuni tipi di dati personali elaborati dagli organi pubblici – e il supporto che li contiene (il registro) – possono essere definiti pubblici dalle leggi speciali (si pensi al registro cantonale dei fiduciari). Pubblici ma non necessariamente liberi: queste leggi possono definire le modalità di elaborazione e di trasmissione, ad esempio il modo di pubblicazione (foglio ufficiale, internet), e definire quando questi dati possono essere visionati (per esempio durante il periodo di pubblicazione) e da chi (ad esempio la consultabilità del catalogo elettorale è limitata ai i soli cittadini aventi diritto di voto).

In sostanza *il diritto della protezione dei dati è l'insieme di tutte le disposizioni che - in un modo o nell'altro – disciplinano l'elaborazione e la trasmissione di informazioni riferite a persone specifiche, che garantiscono l'accesso a queste informazioni a chi ne è legittimato e che impongono l'adozione di misure di protezione, di sicurezza e di controllo*. Queste norme possono riferirsi a rapporti di diritto pubblico in generale (si pensi alla pubblicità del catalogo elettorale), di diritto civile (si pensi alle regole che obbligano il datore di lavoro a trattare i dati del dipendente in quanto si riferiscano all'idoneità lavorativa o siano necessari all'esecuzione del contratto di lavoro) oppure di diritto penale (si pensi alle disposizioni concernenti, segnatamente, la sottrazione di dati personali, l'acquisizione illecita di dati, l'accesso indebito a un sistema per l'elaborazione di dati, il danneggiamento di dati e l'abuso di un impianto per l'elaborazione di dati).

Qualche istante fa avevo parlato di principi-guida della protezione dei dati, che sono contenuti nelle leggi generali (federale e cantonali). Vorrei approfondirli, dando qualche indicazione riferita in merito alle elaborazioni di dati in internet (commercio elettronico e governo elettronico).

➔ Anzitutto è necessario che l'elaborazione di dati personali sia *LECITA*. Con questo concetto si intende, in senso stretto, che l'elaborazione abbia un *fondamento giuridico* valido:

Per le *persone private* vige un principio: chi tratta dati personali non deve ledere *illecitamente* la personalità delle persone interessate. Non può elaborarli in violazione dei principi fondamentali della protezione dei dati (liceità, buona fede, proporzionalità, conformità allo scopo ecc.), non può elaborare i dati di una persona contro la sua esplicita volontà e non può comunicare a terzi dati personali sensibili o profili della personalità. A meno che esista un motivo giustificativo. La legge indica tre categorie di *motivi giustificativi*: una *lesione* è *illecita* se non è giustificata dal *consenso della persona interessata*, da un *interesse preponderante* (privato o pubblico) oppure dalla *legge* medesima. Se non sussiste un motivo giustificativo possono esservi conseguenze di diritto civile (strumenti: azioni e provvedimenti cautelari concernenti la protezione della personalità). Il motivo giustificativo di maggiore rilevanza pratica è il *consenso dell'interessato*, anche nell'ambito del commercio elettronico: questo consenso - e ritornerò sul tema - presuppone un'informazione giusta e completa. Un altro motivo giustificativo di rilievo per i privati è l'*interesse preponderante di chi tratta i dati*. La legge indica alcuni esempi: trattamento in diretta relazione con la conclusione o l'esecuzione di un contratto, nell'ambito di un rapporto di concorrenza economica o della valutazione del credito di una persona (ma a condizioni restrittive), o per scopi impersonali (in particolare nei settori della ricerca, della pianificazione o della statistica). Anche la collezione di dati concernenti persone della vita pubblica (nella misura si riferiscono alla sua attività pubblica) vale come motivo giustificativo. Si può ancora affermare che normalmente non vi è una lesione della personalità se la persona interessata ha reso i dati accessibili a tutti e non si è opposta esplicitamente ad un loro trattamento. Inoltre non è problematica l'elaborazione di dati per uso esclusivamente personale, se i dati non sono comunicati ad estranei.

Per gli *organi pubblici* è invece necessaria una *base legale* o quantomeno – come nel diritto ticinese - che l'elaborazione serva all'adempimento di un compito legale. Queste esigenze assumono contorni più restrittivi qualora l'elaborazione riguardasse dati meritevoli di particolare protezione. Anche lo Stato è evidentemente interessato a pubblicare documenti e informazioni in internet (si pensi ai molteplici progetti dell'e-gov). Se questi contengono dati personali – ma solo in questa misura - sono evidentemente applicabili le disposizioni che reggono la trasmissione di dati. In tal caso è necessario che l'organo responsabile (cioè l'autorità che decide sul contenuto e sul tipo di utilizzazione dei dati, assicurandone il controllo e la gestione) vi sia obbligato o autorizzato dalla legge, oppure - se i dati sono destinati solo ad altri organi pubblici - può essere sufficiente che questi ultimi dimostrino che i dati in quella forma siano necessari per l'adempimento dei loro compiti legali. Il diritto federale è ancora più preciso ed esigente, poiché prevede che una pubblicazione di dati personali in internet, curata da organi federali, necessita di una base legale esplicita. In effetti questa forma di pubblicazione è qualificata come una comunicazione di dati mediante procedura di richiamo: addirittura, dati sensibili possono essere resi accessibili mediante una procedura di richiamo soltanto qualora lo preveda esplicitamente una base legale in senso formale.

➔ Un altro principio guida è quello della *PROPORZIONALITÀ*, determinante sia per i privati che per l'ente pubblico. Secondo questa massima, possono essere raccolti ed elaborati solo i dati personali *idonei e necessari* allo scopo (che dev'essere a sua volta lecito). La lesione della personalità dev'essere, infine, in un *rapporto ragionevole con lo scopo perseguito*.

Nell'ambito dell'e-commerce sono sovente necessarie meno informazioni personali di quelle che invece vengono in realtà raccolte nella mascherina d'introduzione dei dati. Nella misura del possibile bisognerebbe pure rinunciare a richiedere - e raccogliere - dati sensibili oppure dati superflui. In definitiva, visto che ogni raccolta ed elaborazione di dati dev'essere esaminata dal profilo della proporzionalità, sarebbe opportuno prevedere soluzioni personalizzate per offrire al cliente un'assistenza ottimale. Questo principio vale anche per gli organi pubblici. Ogni progetto di e-government che esige la pubblicazione di dati personali deve rispettare il principio della proporzionalità: in tal senso, devono essere divulgati solo i dati idonei e necessari ai fini dello scopo perseguito.

➔ Il principio della *BUONA FEDE*, altro principio guida, esige una raccolta ed elaborazione di dati *trasparente* e *leale*. Questa massima intende tutelare la volontarietà della messa a disposizione di informazioni personali. I dati non possono essere raccolti sottacendo fatti inveritieri né utilizzati in modo inatteso per un altro scopo. Viola poi questo principio l'indicazione ambigua o non trasparente dello scopo della raccolta e dell'elaborazione dei dati.

Nell'ambito dell'e-commerce la raccolta e l'elaborazione di dati devono essere riconoscibili e leali, anche perché il profilo del cliente consente una connessione di dati personali, con la quale è possibile ottenere informazioni completamente nuove sul suo conto. Indicazioni generiche come "raccolta di dati per scopi amministrativi" dicono veramente poco e sono quindi assolutamente sconsigliabili, qualora invece il loro scopo reale fosse quello di valutarli anche in prospettiva di un'analisi approfondita del profilo del cliente. Anche l'ente pubblico, ed è persino ovvio, deve utilizzare i dati raccolti solo in conformità a detto principio, in stretta connessione con lo scopo perseguito.

➔ Proprio il *VINCOLO*, la *CONFORMITÀ ALLO SCOPO* è un'altra massima assolutamente significativa – strettamente legata alle precedenti - ed impone a chi elabora i dati di trattarli soltanto per lo scopo indicato all'atto della loro raccolta, oppure che risulti dalle circostanze o sia previsto dalla legge. È richiesta quindi una chiara definizione dello scopo. Per i rapporti tra privati, una successiva modifica dello scopo deve, di principio, avvenire solo con il consenso della persona interessata, oppure, per gli organi pubblici, con l'adozione di una base legale. Raggiunto lo scopo, i dati non più necessari devono di principio essere eliminati.

Nell'ambito del commercio elettronico, sapere se una raccolta di dati personali sia conforme allo scopo, è una questione che può essere esaminata solo di caso in caso. Per coloro che fanno capo alle prestazioni dell'e-shop dovrebbe essere chiaro, in generale, che lasciano tracce di dati, tecnicamente utilizzabili per favorire un'assistenza puntuale. Tuttavia la quantità dei dati elaborati è sovente molto superiore a quanto il cliente possa immaginare. Anche se lo scopo dell'elaborazione di dati è spesso riconoscibile dalle circostanze del caso specifico, si consiglia di informare sempre e in modo chiaro e completo sullo scopo perseguito. Un'elaborazione di dati che non sia più compatibile con lo scopo originario, per esempio la trasmissione a terzi, presuppone di norma il consenso della

persona interessata. A questo principio è vincolato anche l'ente pubblico, che però ha a disposizione lo strumento della legge per precisare gli scopi e definire eventuali destinatari. La condizione posta dal diritto cantonale è di non utilizzare i dati in modo incompatibile con quello per i quali sono stati raccolti.

➔ In tutto questo contesto, i principi illustrati sono strettamente connessi tra loro e sono anche il fondamento di due altre massime, il principio dell'*ESATTEZZA DEI DATI* (i dati devono essere esatti e, nella misura in cui lo scopo dell'elaborazione lo richieda, completi; quindi vi è un obbligo di chi tratta i dati di accertarsi della loro esattezza) e il principio della *SICUREZZA DEI DATI* (chi li elabora deve prendere misure tecniche ed organizzative appropriate contro la perdita, il furto, l'elaborazione e la consultazione illecite). Lo scopo della sicurezza è di garantire la confidenzialità, la disponibilità e l'integrità dei dati per proteggerli adeguatamente. I rischi principali sono la distruzione accidentale o non autorizzata dei dati, gli errori tecnici, la falsificazione, il furto e l'uso illecito, ma anche la modificazione, la copia, l'accesso o altro trattamento non autorizzato. Le misure tecniche e organizzative devono essere appropriate, a dipendenza dello scopo, della natura e dell'estensione del trattamento. La valutazione dei rischi potenziali per le persone interessate e lo sviluppo tecnico vanno anche considerati. In materia di sicurezza dei dati l'Incaricato federale per la protezione dei dati ha pubblicato interessanti opuscoli divulgativi, scaribili dal suo sito www.edsb.ch.

➔ Cosa traspare dall'insieme di questi princìpi con riferimento particolare ad internet? In sostanza, i detentori di raccolte di dati personali devono creare i presupposti - certo tecnici ed organizzativi - ma soprattutto legali per consentire alle persone interessate di autodeterminarsi sulle elaborazioni di dati che le concernono e per esigere che i loro dati siano trattati in modo lecito, leale e trasparente. Per promuoverne il rispetto, la legge contiene diritti dell'utenza e, come corollario, doveri per chi elabora i dati, che possono riassumersi in diritti e obblighi d'informazione.

2.4. Diritti e obblighi d'informazione oggi

Sia per i privati sia per gli organi pubblici, sia a livello federale che cantonale, le leggi generali sulla protezione dei dati sanciscono una prerogativa - non certo l'unica - ma sicuramente la più importante: il *DIRITTO D'INFORMAZIONE* o *D'ACCESSO*, valido anche

per i dati personali elaborati in internet. Il diritto d'accesso consente alla persona interessata di domandare al detentore di una collezione di dati di comunicarle se e quali informazioni che la concernono sono trattati. E il detentore ha l'obbligo di fornirle, affinché la persona interessata possa richiederne – se lo desidera e se le condizioni legali sono soddisfatte - la cancellazione, la rettifica o esigere il blocco della trasmissione a terzi. L'informazione è di regola gratuita e scritta secondo il diritto federale, mentre da parte di organi pubblici cantonali e comunali l'informazione avviene in forma scritta solo su richiesta. Il diritto d'accesso non è assoluto, ma – a precise e restrittive condizioni - può essere limitato, differito o addirittura rifiutato, in particolare se lo esigano interessi preponderanti privati o pubblici.

Nell'ambito del commercio elettronico, questo diritto dell'utente obbliga il detentore di una raccolta di dati personali a creare le premesse tecniche, organizzative e procedurali affinché la persona interessata possa ottenere visione delle informazioni personali che la riguardino. La banca dati dev'essere strutturata in modo tale che, su richiesta, tutte le informazioni registrate su una persona determinata possano essere agevolmente cancellate, rettificate o bloccate nei confronti di terzi. Per le informazioni detenute dagli organi pubblici il discorso è evidentemente un po' diverso. Questi diritti esistono certamente, ma la loro portata va raffrontata alla necessità per lo Stato di adempiere i compiti legali, chiamato sovente a raccogliere ed elaborare i dati personali dei cittadini.

Il diritto d'informazione non è immediato; occorre farlo valere, all'occorrenza davanti al giudice. Nell'odierna società dell'informazione e considerata la spontaneità del flusso di informazioni in internet, potrebbe anche rivelarsi non pienamente efficace dal profilo pratico, ad esempio se le persone interessate non fossero a conoscenza dell'esistenza di una raccolta di dati, né dei suoi elementi determinanti. Più utili potrebbero invece rivelarsi altre misure – che peraltro già esistono – ma che vanno accresciute e rafforzate, a tutto vantaggio della trasparenza e della lealtà nei rapporti tra elaboratori di dati e utenti.

L'Incaricato federale per la protezione dei dati ha già avuto modo di sottolineare la necessità di aumentare la trasparenza delle elaborazioni di dati in internet per garantire meglio la tutela della personalità. Rivolgendosi ai fornitori di servizi internet, ha chiesto loro di migliorare la politica d'informazione, considerate le possibilità assai agevoli di raccogliere le informazioni sulla base delle visite effettuate su internet e di elaborarle ai fini

di studi di mercato o anche di venderle a terzi. L'Incaricato ha quindi suggerito l'adozione di alcune misure – da riassumere in un modulo di avviso, internazionalmente noto come *"informativa sulla riservatezza o sulla privacy",* e precisamente:

- segnalare in un posto ben visibile del sito internet le basi legali di protezione dei dati applicabili all'offerta. L'indicazione dev'essere presentata in modo chiaro, specificando in particolare quali dati saranno raccolti e utilizzati e a quale scopo;

- dare all'utilizzatore la possibilità di limitare l'elaborazione di dati (p.es. se si oppone all'elaborazione del suo profilo di consumatore) e la trasmissione di dati che lo riguardino (p.es. a fini pubblicitari);

- secondo la destinazione dei dati, adottare misure di sicurezza che possano garantire la confidenzialità, l'esattezza, l'integralità e l'attualità dei dati (p. es. metodi di criptaggio e di autentificazione);

- infine, indicare il modo con cui l'utilizzatore può far valere i propri diritti.

Queste raccomandazioni – senza dubbio giuste - trovano però ancora un riscontro insufficiente nella pratica del nostro Paese. Consultando i siti internet, queste informative, se esistono (a differenza dell'Italia, dove vige un obbligo specifico), non sono sempre molto strutturate. Vi sono però lodevoli eccezioni, frutto più che altro dell'autodisciplina di singoli fornitori di servizi. Per esigere un'informativa compiuta occorre una revisione legislativa, una revisione che imponga *un obbligo attivo d'informazione*.

2.5. Diritti e obblighi d'informazione domani

Questa revisione è in corso. Il 19 febbraio scorso il Consiglio federale ha licenziato un messaggio corposo con cui intende proporre alle Camere federali di adattare la legge federale sulla protezione dei dati, in primo luogo – ma non solo - proprio allo scopo di migliorare l'informazione delle persone i cui dati sono raccolti. Questo esame è attualmente al vaglio della Commissione degli affari giuridici del Consiglio nazionale, che 9 giorni fa è entrata in materia. Cosa prevede concretamente questa revisione? In tre concetti: *riconoscibilità*, *consenso*, *informazione attiva*.

Il disegno non si scosta dalla concezione, prevalente finora, che lascia principalmente alla persona interessata l'iniziativa di far valere e di difendere i propri diritti, tra cui quello d'accesso. Ma se l'utente avrà la possibilità di sapere già all'atto della raccolta se e quali dati saranno raccolti sul suo conto, sarà ancora più facile per lui decidere fino a che punto vorrà tollerare eventuali lesioni alla sua sfera privata, rafforzando così la responsabilità e la diligenza dei detentori di raccolte di dati. In definitiva, il messaggio è finalizzato a promuovere meccanismi di autodisciplina e di autoregolamentazione, non da ultimo con l'assegnazione di marchi di qualità e certificazioni nella protezione dei dati. E queste sono altre interessanti e importanti novità proposte con la revisione.

Per quanto concerne esplicitamente l'informazione, il disegno sancisce il principio secondo il quale la raccolta deve essere *riconoscibile*, in particolare per quanto attiene alle sue finalità. Questo principio legale – completamente nuovo per le elaborazioni di date da parte di persone private – è completato da un *obbligo di informare circostanziato* per i dati personali sensibili e i profili della personalità.

➔ Le esigenze legate alla *RICONOSCIBILITÀ* di un'elaborazione di dati vanno valutate a seconda delle circostanze, in base ai principi della buona fede e della proporzionalità. Si tratterà in particolare, nella prassi, di esaminare se in una determinata situazione questi principi esigano che il detentore di una raccolta di dati attiri l'attenzione dell'utente con mezzi appropriati, non soltanto sull'esistenza della collezione, ma anche sui suoi elementi determinanti, come lo scopo, l'identità del detentore o le categorie di destinatari dei dati qualora si pensi a una loro comunicazione. Ecco alcuni esempi, tratti dal messaggio: se in caso di richiesta di una carta cliente si devono indicare dati personali è evidente che la ditta li utilizzerà per inviare al cliente la propria pubblicità. Tuttavia, se l'uso della carta consente di raccogliere dati sulle abitudini del cliente, per allestire profili dei consumatori o venderli a terzi, i clienti devono essere adeguatamente informati (p.es. mediante una corrispondente osservazione sul modulo di richiesta). Per le transazioni semplici, in cui sono facilmente riconoscibili le finalità e l'identità dei detentori, non vi sono previsti nuovi obblighi particolari.

➔ Il disegno di legge chiarisce anche la nozione e la portata del *CONSENSO*. Quando l'elaborazione di dati è subordinata al consenso della persona interessata, il consenso è valido soltanto se espresso liberamente e dopo debita informazione. Trattandosi di dati

sensibili, il consenso dev'essere esplicito. Questa nuova disciplina è un'importante conquista. La persona interessta deve essere informata delle conseguenze negative o degli svantaggi che potrebbero risultare da un rifiuto. È comunque determinante il principio della proporzionalità commisurato alla qualità dei dati: più i dati sono sensibili, più le esigenze al consenso devono essere chiare.

➔ L'*OBBLIGO ATTIVO DI INFORMARE* va oltre l'esigenza della riconoscibilità, illustrata poco fa. L'informazione deve avvenire d'ufficio, ma unicamente per la categoria dei dati sensibili e dei profili della personalità. Questa maggiore tutela del singolo si fonda sul concetto di prevenzione e tende a migliorare l'efficacia dei principi guida. Così, se deve informare in modo più circostanziato, il detentore della raccolta di dati avrà interesse a non raccogliere, registrare e comunicare dati sensibili non assolutamente necessari. *Oggetto* di quest'obbligo sono tutte le informazioni necessarie. Se la buona fede lo esige, dovrà fornire ulteriori indicazioni, per esempio sul carattere obbligatorio o facoltativo della raccolta o sulle conseguenze del rifiuto di rispondere. L'informazione non è subordinata a particolari *esigenze di forma*, quindi un'indicazione verbale potrebbe bastare, come anche un'informazione data su un supporto separato o esposta in un luogo ben visibile (si pensi all'affissione, a un testo allegato alla fattura, ad una rubrica ben visibile sulla home page di internet). Determinante è che sia sufficientemente visibile, leggibile e comprensibile. Se è prevista una comunicazione di dati, la persona interessata può essere resa attenta con una clausola che la invita ad autorizzare o rifiutare la comunicazione. In questo modo il detentore dei dati è sicuro che l'interessato è stato compiutamente informato. Ad esempio una cassa malati deve informare esplicitamente – con una lettera o un contratto – in che modo sono utilizzati i dati di salute dell'assicurato a cui può accedere.

Nell'ambito del commercio elettronico questo obbligo attivo e accresciuto di informazione nei confronti dei clienti e dei navigatori è molto importante. In fondo è poi anche nell'interesse dei singoli fornitori di servizi adottare tali misure se intendono assicurarsi la fiducia dei consumatori. In sostanza, la persona interessata deve essere informata attivamente perlomeno sull'identità del detentore della raccolta di dati, sullo scopo dell'elaborazione e sulle categorie di eventuali destinatari di dati (non sui singoli destinatari). Se il principio della buona fede lo esige, il detentore deve rilasciare ulteriori informazioni. Quest'obbligo di informazione può essere attuato nelle condizioni generali di con-

tratto oppure nell'informativa del sito internet. Ad esempio, l'indicazione nella home page di una rubrica sufficientemente visibile che rinvia a informazioni riguardanti la raccolta e l'utilizzazione di dati dovrebbe costituire normalmente un mezzo semplice e adeguato per attirare l'attenzione della persona interessata. Anche l'indicazione su un modulo di un avviso che, salvo opposizione da parte della persona interessata, i dati saranno comunicati a scopo di ricerca di mercato o per altri scopi può apparire sufficiente. Se la raccolta di dati è facoltativa, una clausola che permette alla persona interessata di esprimere il proprio consenso (anche se non formalmente richiesto dalla legge) evita verosimilmente molti problemi, visto che il detentore è certo della riconoscibilità della raccolta e del consenso della persona interessata. È però auspicabile, d'altra parte, che queste clausole garantiscano all'utenza anche una reale possibilità di scelta, senza privarla di servizi qualora non fosse d'accordo a rilasciare i propri dati. Attualmente si assiste a questo tipo di speculazioni.

Per esigere il rispetto dell'obbligo d'informazione, il disegno di legge prevede una nuova *sanzione penale*, che sanziona, a querela di parte, con l'arresto o con la multa le persone private che contravvengono agli obblighi d'informazione fornendo intenzionalmente informazioni inesatte o incomplete, e omettendo intenzionalmente di informare le persone interessate.

Solo il tempo e l'esperienza sapranno rivelare gli effetti di tutte queste misure.

3. Conclusione: autodisciplina, trasparenza e informazione quali premesse della privacy

In conclusione, la tutela della riservatezza non nega affatto l'importanza, la necessità e il valore della circolazione di dati personali nella nostra società, viepiù globalizzata, ma tende ad assicurare già dal momento della raccolta di queste informazioni, il rispetto della libertà delle persone e della loro dignità, che sono garantite costituzionalmente. Uno strumento - direi importante, anzi essenziale - oltre alle varie leggi, è la *singola autodisciplina di chi elabora i dati altrui*, affinché li tratti solo in quanto necessario e in modalità trasparenti e leali. Per promuovere questa autodisciplina è determinante l'affermazione di un *obbligo attivo d'informare* nell'ambito della raccolta e della gestione di dati personali.

Se le Camere federali approveranno la modifica proposta dal Consiglio federale, la legge federale sulla protezione dei dati conterrà – in questo senso - *precisi obblighi a carico di chi elaborerà dati personali*, anche in internet. Questa modifica va indubbiamente nella direzione giusta. Peccato però che il Consiglio federale abbia rinunciato ad estendere questi vincoli ad ogni raccolta di dati personali, per limitarli alla sola categoria – peraltro la più delicata – dei dati sensibili e dei profili della personalità. Questi obblighi sono già sanciti dal diritto comunitario e dalle raccomandazioni del Consiglio d'Europa, sicché non è esclusa in futuro una loro ulteriore estensione.

In definitiva, *chiarezza*, *trasparenza* e *informazione* devono assurgere a veri e propri cardini del rapporto tra tutela della personalità e circolazione di informazioni nel mondo globale, come premesse fondamentali per la sicurezza dei dati.

Ma in realtà – e mi ricollego a quanto esposto all'inizio - occorre anche fare appello alla *responsabilità del singolo utente*, poiché (spesso istintivamente, ma spesso anche coscientemente) non si preoccupa di fornire qualsiasi tipo di dati personali, soprattutto in internet: il suo numero di carta di credito, la sua data di nascita, la sua professione e via dicendo. In molte homepages si leggono curriculi personali, nelle chatrooms si divulgano fatti intimi. Anche con questi dati, o meglio con la combinazione di tutti queste informazioni (con un po' di abilità e un buon motore di ricerca), è possibile ricavare profili personali. E non solo in internet: in molti formulari si richiedono moltitudini di dati, oggettivamente superflui. Se si hanno dubbi, non costa nulla chiedere le ragioni per cui determinati dati vengono raccolti. Va ricordato che in ultima analisi ognuno è responsabile di ciò che divulga su se stesso, cosicché non si può che sottolineare, anche in questo contesto, l'importanza dell'autodisciplina.

Solo con la collaborazione di tutti gli attori, cominciando da loro stessi e da chi elabora i dati, è possibile creare le premesse per ridare idealmente al concetto universale di privacy, di autodeterminazione, *il suo senso più vero*, non certo per facilitare il compito delle autorità di controllo e di vigilanza, ma per accrescere la "fiducia globale" nell'utilizzo dei moderni strumenti di comunicazione telematica.

Vi ringrazio.