ICT E DIRITTO

Rubrica a cura di

Antonio Piva, David D'Agostini

Scopo di questa rubrica è di illustrare al lettore, in brevi articoli, le tematiche giuridiche più significative del settore ICT: dalla tutela del *domain name* al *copyright* nella rete, dalle licenze software alla *privacy* nell'era digitale. Ogni numero tratterà un argomento, inquadrandolo nel contesto normativo e focalizzandone gli aspetti di informatica giuridica.

10 anni di Privacy: la protezione dei dati personali tra passato e futuro

Leonardo Felician, David D'Agostini, Antonio Piva

1. Introduzione

Da quando ha fatto la sua prima comparsa in Italia esattamente dieci anni fa, il 6 maggio 1997, la tutela della privacy ha acquistato uno spessore, un'articolazione e un'importanza crescenti, entrando nella vita di ciascuno - privati e aziende - e modificandone in positivo gli stili di comportamento. Ultima in Europa - la Francia con la *Commission Nazionale Informatique et Libertées* e la Germania con la *Datenschutzgesetz* si erano dotate di una regolamentazione in materia di privacy una dozzina di anni prima - l'Italia approvava la legge 675 il 31 dicembre 1996, una data alquanto insolita per un argomento che era in discussione in Parlamento dalla metà degli anni '80, con numerosi disegni di legge e commissioni di studio guidate dai più noti giuristi dell'epoca, da Mirabelli a Picano.
L'urgenza era conseguenza del termine ultimo fissato dagli accordi di Schengen: senza una legge a tutela dei dati personali l'Italia non sarebbe potuta entrare nello spazio comune europeo previsto dagli accordi, in quanto per costituire un'area unica in cui si trasferiscono persone, merci, informazioni senza controlli è indispensabile che i confini siano tutelati e che - nel caso specifico - i dati personali non possano uscire se non nelle maniere previste. Questo stesso principio vale oggi per i nuovi Stati membri dell'Unione Europea, che hanno tutti più o meno adottato normative conformi, ispirate alla Direttiva Comunitaria 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.
Per recepire in maniera propria questa direttiva, oltre che per riformulare la materia dopo lunghi anni di comunicati stampa, interpretazioni, correzioni e confronti con tutte le realtà produttive e associative, il ponderoso lavoro svolto dall'Autorità Garante[1] consegnò alla *Gazzetta Ufficiale* il 29 luglio del 2003 il nuovo Codice in materia di Protezione di dati personali, emanato con Decreto Legislativo 196 del 20/6/03 che in tre parti, 56 capitoli e ben 186 articoli, riordina e disciplina una materia che tocca cittadini e aziende, associazioni ed enti, giovani e vecchi, e perfino defunti e nascituri, perché la disciplina sulla privacy è pervasiva e riguarda tutti i cittadini del nostro Paese.
Il Codice è entrato in vigore in Italia dal primo gennaio 2004, data di abrogazione della celebre legge 675/96. Le fonti normative su cui si basa sono numerose ed importanti: la Costituzione Italiana, la Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950, la Convenzione 108 sulla protezione delle persone nel trattamento automatizzato di dati a carattere personale (1981) e la sua ratifica nella legge 98/89, gli Accordi di Schengen del 1985, la Convenzione per la loro applicazione (1990) e ratifica nella Legge 388/93, nonché due fondamentali Direttive comunitarie, la 95/46/CE relativa alla tutela delle per-

[1] www.garanteprivacy.it

sone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati e la già citata Direttiva 2002/58/CE.
Poche leggi hanno inciso in maniera così significativa in così poco tempo quanto a modi di comportarsi e procedure operative: è passata tanta acqua sotto i ponti dal famoso caso BNL quando il Garante ebbe modo di dare un segno forte e chiaro per far capire che lo spirito della legge era più importante della burocrazia ribilanciando così l'arroganza delle banche nei confronti dei clienti[2], con l'introduzione già allora del fruttuoso concetto di *consenso differenziato*[3].
L'interesse e la vastità dell'argomento con tutte le sue articolazioni è testimoniato anche dalla frequenza e dal numero di pubblicazioni[4] e di convegni sulla privacy ospitati in questi anni, che hanno puntualizzato diversi aspetti utili alle imprese di tutte le dimensioni, tutti volti a trovare modelli operativi semplici, ma rispettosi dello spirito della legge. Questo è un altro degli aspetti peculiari di questa normativa: l'applicazione non burocratica, ottusa e scolpita nella pietra, ma al contrario flessibile e intelligente, aperta al dialogo con le realtà produttive, in grado di adeguarsi in maniera dinamica ad una realtà tecnologica che cambia di giorno in giorno.

2. Principi generali

La complessità tecnica della legge sulla privacy, dietro cui si trincerano spesso i denigratori, scompare se si tengono presenti i grandi principi cui essa si ispira, esposti con chiarezza nei primi articoli: l'art. 1 definisce che la protezione dei dati personali è un diritto soggettivo, mentre l'art. 2 illustra le finalità e garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza e all'identità personale.
Possono sembrare affermazioni generiche, ma spesso sono proprio questi principi a costituire il faro che orienta tra trattamenti leciti e non leciti: nel pensiero del Garante in tutti questi anni è stata proprio questa la bussola per le decisioni più sofferte. Il bilanciamento della difesa di diritti dello stesso rango è un'arte difficile, quando la privacy si contrappone al diritto alla vita, al diritto alla sicurezza e alle misure antiterrorismo o al diritto di cronaca e alla libertà di stampa.
L'art. 3 stabilisce il principio di necessità e chiede di trattare i dati in forma anonima laddove non sia strettamente necessario trattare dati identificativi[5]. Nell'art. 4 si trovano le principali definizioni, tra le quali va ricordato che un *dato personale* è qualunque informazione relativa a persona fisica, giuridica, ente o associazione identificata o identificabile mediante riferimento a qualsiasi altra informazione, mentre per *trattamento* si intende qualunque operazione o complesso di operazioni con o senza l'ausilio di strumenti elettronici. L'art. 5 infine definisce l'ambito di applicazione della legge, che riguarda tutti i trattamenti effettuati da chiunque sia stabilito nel territorio italiano oppure - se stabilito fuori dall'Unione Europea - impieghi strumenti situati nel territorio italiano. Il terzo comma mette in luce un'importante eccezione: non ricadono sotto le previsioni di questa legge i trattamenti effettuati da persone fisiche per fini esclusivamente personali senza comunicazione sistematica o diffusione.
L'impianto che è stato dato a questo monumentale testo unico fa sì che la prima parte, *Disposizioni generali*, indichi regole generali che

[2] BNL aveva consegnato ai suoi correntisti un'informativa sui dati personali che richiedeva un consenso incondizionato al trattamento anche a fini promozionali, minacciando la chiusura del conto corrente in caso di diniego. Il Garante intervenendo con tempestività nell'arco di pochi giorni a fine aprile 1996 chiarì che detto comportamento era contro la legge, obbligò la banca a riscrivere l'informativa e a sottoporla prima di reinviarla a centinaia di migliaia di correntisti. Il Garante concluse la sua ferma presa di posizione su questo caso, ampiamente citato e reso noto, affermando che non dava seguito a sanzioni, soltanto a motivo del fatto che la legge non era ancora tecnicamente in vigore. Il messaggio fu sufficiente per tutte le banche e le grandi aziende italiane per comprendere che la nuova legge andava presa sul serio.

[3] È ormai prassi comune chiedere il consenso per i trattamenti obbligatori, senza il quale non è possibile instaurare rapporti o servizi, e il separato consenso per il trattamento a fini promozionali, commerciali o di ricerche di mercato, la cui mancata autorizzazione non comporta conseguenze di sorta.

[4] Anche su questa rivista: si veda Mondo Digitale n. 1, marzo 2004.

[5] Indicando che i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzo di dati personali e di dati identificativi.

riguardano tutti, mentre la seconda parte introduce con estremo dettaglio le disposizioni particolari per specifici settori (giudiziario, pubblico, sanitario, bancario, finanziario ecc.); la terza parte, infine, riporta le norme per la tutela amministrativa e giurisdizionale e il funzionamento dell'Ufficio del Garante.
L'art. 7 stabilisce i fondamentali diritti di ciascuno rispetto ai dati personali che lo riguardano, pertanto risulta opportuno esaminarlo dal duplice punto di vista del cittadino e di chi opera in azienda. A semplice richiesta, senza formalità e con risposta non oltre 15 giorni l'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano e la loro completa comunicazione in forma intelligibile. Inoltre l'interessato ha diritto di ottenere l'indicazione:

- dell'origine dei dati personali;
- delle finalità e delle modalità del trattamento;
- degli estremi del Titolare e dei responsabili;
- dei soggetti o categorie di soggetti ai quali i dati personali possono essere comunicati;
- dell'aggiornamento, rettifica o integrazione dei dati;
- della cancellazione, trasformazione in forma anonima o blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati.

Quest'ultimo diritto è tuttora poco conosciuto e mal interpretato: non è possibile infatti chiedere incondizionatamente, come spesso succede, la cancellazione dei propri dati personali, perché se questi sono stati acquisiti in modo lecito e trattati secondo la legge, nemmeno il Garante può obbligare un'impresa o un ente a cancellarli. Spesso questo punto è frainteso con un ultimo diritto, questo sì incondizionato e non assoggettabile ad alcun vincolo o costo, e cioè quello di vietare comunicazioni pubblicitarie, di vendita diretta, di ricerche di mercato o commerciali, in altre parole il diritto a non essere inutilmente disturbati.
L'art. 11 stabilisce che i dati personali oggetto di trattamento devono essere:

- trattati in modo lecito e secondo correttezza;
- trattati per scopi determinati, espliciti e legittimi;
- esatti e se necessario aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità;
- conservati per un periodo non superiore al necessario.

Quest'ultimo punto è molto controverso: cancellare i dati trascorso il periodo del loro ragionevole utilizzo è senz'altro nello spirito della legge, ma al di là delle (superabili) difficoltà tecniche, ciò cancellerebbe la storia. L'indicazione del Garante trova una vasta resistenza all'interno di qualunque impresa o ente: è inevitabile che su questo punto, ancora aperto, al di là delle affermazioni di principio si giunga a una definizione più precisa di cosa è lecito conservare -e non in forma anonima- per fini storici e di documentazione.
L'art. 13 della legge riguarda l'informativa che deve essere obbligatoriamente resa all'interessato, in forma scritta oppure orale (laddove possibile le aziende hanno sempre preferito la forma scritta, sia per documentazione, sia perché minimizza i costi) prima di cominciare a trattare i suoi dati. In essa devono essere descritte le finalità e le modalità del trattamento, la natura obbligatoria o facoltativa del conferimento, la conseguenza al rifiuto di rispondere, i soggetti o categorie di soggetti cui possono essere comunicati i dati e il loro ambito di diffusione, i diritti di cui all'art. 7, gli estremi identificativi del Titolare e dei Responsabili[6].
Per i dati raccolti presso l'interessato l'informativa va data subito, mentre per i dati raccolti a distanza o presso terzi essa va data non oltre la prima comunicazione. Non basta però consegnare l'informativa, è necessario anche raccogliere il consenso prima di procedere al trattamento, con importanti differenze tra i dati comuni e i dati giudiziari e sensibili, oggetto di maggiore tutela. Questi ultimi sono dati idonei a rilevare l'origine razziale ed etnica, le opinioni politiche, l'adesione a partiti, sindacati, associazioni, organizzazioni, lo stato di salute e la vita sessuale di una persona. Il trattamento dei dati comuni è possibile con il *consenso*, documentato per iscritto (art. 23), espresso liberamente e specificamente per un trattamento chiaramente individuato. Nell'ipotesi, non infrequente, di trattamento e rac-

[6] Il principio dell'informativa sottintende il concetto di trasparenza. Infatti l'interessato deve essere edotto chiaramente ed esaustivamente, preventivamente al conferimento, su tutti quegli elementi che coinvolgono il trattamento dei suoi dati personali.

colta dei dati mediante sito internet, la preventiva informativa dovrà essere posizionata in modo chiaramente visibile, ed il consenso potrà essere espresso tramite compilazione di un *form*[7] e successivamente memorizzato in ottemperanza all'obbligo di documentazione.
Sono previsti inoltre alcuni casi di esonero dal consenso, tra i quali due molto importanti e frequenti. Il consenso infatti non è necessario ai sensi dell'art. 24:

- per trattamenti derivanti da obblighi di direttiva comunitaria, legge, regolamento, normativa;
- per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione dello stesso, a specifiche richieste dell'interessato.

Se pertanto, per fare un esempio, una persona telefona comunicando i propri dati al fine di ottenere un preventivo per una prestazione, tali dati possono essere trattati, dopo aver fornito l'informativa, in esenzione da consenso[8].
Il trattamento dei dati sensibili, invece, è possibile solo previa autorizzazione del Garante e con il consenso espresso, senza deroghe, in forma scritta[9]. Di fatto il Garante ha fatto ampio uso delle cosiddette autorizzazioni per categoria, permettendo di trattare determinate specie di dati sensibili a una serie di soggetti che ne fanno normalmente uso (per esempio, trattamento di dati sanitari per chi esercisce la professione medica). Il principio che si evince è che l'intervento del Garante deve essere per eccezione, mentre i casi comuni devono ricadere nella normativa: il tempo aiuta a far evolvere la normativa stessa verso una razionalizzazione e una semplificazione auspicata da più parti, ma spesso anticipata dal Garante stesso. A questo proposito l'art. 26 ha recepito un unico importante caso di esonero dal consenso per il trattamento dei dati sensibili, che riguarda i rapporti di lavoro. Chiunque abbia dipendenti e debba dunque trattare dati inerenti la loro salute ed eventualmente la loro associazione a sindacati, può farlo anche in assenza del consenso del lavoratore. Il Garante, dal canto suo, ha dimostrato attenzione alle ipotesi in cui il trattamento è dovuto in forza di altre leggi: un esempio riguarda la richiesta di risarcimento per lesioni in un sinistro: la compagnia di assicurazioni ha la necessità di trattare dati sensibili e chiede il consenso dell'interessato, ma in assenza non può semplicemente rifiutarsi di trattare i dati e quindi di risarcire il sinistro, in quanto vi è tenuta in forza di altra legge (nell'esempio il Codice delle assicurazioni approvato con D. Lgs. 209/05).
Da ultimo va sottolineato che comunicazione (*dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma*, per esempio, scrivendo o comunicando a voce) e diffusione (*dare conoscenza dei dati a soggetti indeterminati, in qualunque forma*, per esempio, pubblicando su un sito internet) dei dati sono trattamenti ammessi con il consenso espresso dell'Interessato, con l'unico esonero delle comunicazioni in forza di obblighi di legge.
Non è vero, dunque, che questa legge impedisca o limiti il trattamento dei dati: vero è che lo disciplina, lo chiarisce e lo fa emergere da quella zona di grigio in cui a taluni farebbe comodo mantenerlo. Poco a poco (anche per l'opera di un maestro rigoroso dallo stile personale e molto diretto come è stato per otto anni nei suoi due mandati il prof. Stefano Rodotà, primo presidente dell'Autorità Garante per la privacy in Italia) le aziende, ma anche i mass media e i cittadini hanno cominciato a comprendere la portata della legge e ad applicarla in maniera corretta. Proprio Rodotà, che è stato anche presidente dei Garanti Europei, sosteneva spesso che nei paesi evoluti, la correttezza nel trattamento dei dati personali è un vantaggio competitivo che qualifica le aziende migliori e che un pubblico di consumatori educati è capace di apprezzare la diffe-

---

7 Con la possibilità di scegliere se accettare attraverso opportune caselle selezionabili dall'interessato.

8 Sostanzialmente l'interessato può esprimere il proprio consenso anche oralmente; è utile che il soggetto che raccoglie i dati abbia cura di documentare per iscritto la manifestazione della volontà, oppure che sia stata stabilita una procedura automatica che dimostri detta manifestazione, per esempio, un albero vocale che prima di passare alla transazione chieda esplicitamente di fornire il consenso mediante pressione di un tasto.

9 In questo caso, mediante raccolta attraverso e-mail o web, il requisito della forma scritta rende possibile la sottoscrizione del consenso solamente mediante firma elettronica conforme alle normative vigenti in materia, che peraltro è in continua evoluzione e potrebbe trovare altre forme ammissibili, data la scarsissima diffusione della firma digitale in Italia.

renza tra gli operatori sul mercato e premiare quelli maggiormente rigorosi.

3. Tecnologie, nuovi aspetti problematici e il Garante

La tecnologia apre però sempre nuovi fronti: dalle etichette RFID alla videosorveglianza, dalla privacy delle e-mail al diritto di cronaca; l'Autorità Garante è intervenuta più volte anche dopo l'ingresso in vigore del Codice Privacy. Con provvedimento generale del 1° marzo 2007 sono state dettate le linee guida in relazione all'utilizzo della posta elettronica e della rete internet sul posto di lavoro: premesso il diritto (e l'obbligo normativo) del datore di lavoro di adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità dei propri sistemi informativi e di dati, risulta necessario approntare una tutela per i lavoratori di fronte al rischio di controlli della corrispondenza elettronica e della navigazione sul web. La soluzione suggerita passa attraverso l'adozione di un disciplinare aziendale redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori mediante opportuna formazione ed informazione, attraverso rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori ecc.) e da sottoporre ad aggiornamento periodico. A seconda dei casi andrebbe per esempio specificato:

- quali comportamenti non sono tollerati rispetto alla "navigazione" in internet (per esempio, il *download* di *software* o di *file* musicali), oppure alla tenuta di file nella rete interna;
- in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di *webmail*, indicandone le modalità e l'arco temporale di utilizzo (per esempio, fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
- quali informazioni sono memorizzate temporaneamente (per esempio, le componenti di *file* di *log* eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;
- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di *back up*, della gestione tecnica della rete o di *file* di *log*);
- se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime, specifiche e non generiche, per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete internet sono utilizzate indebitamente;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;
- se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato;
- quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi (*art. 34 del Codice, nonché Allegato B*), *in particolare regole 4, 9, 10*).

Il Garante, inoltre, ha vietato ai datori di lavoro di effettuare trattamenti di dati personali mediante sistemi *hardware* e *software* che mirano al controllo a distanza di lavoratori, svolti in particolare mediante:

a. la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
b. la riproduzione e l'eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
c. la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
d. l'analisi occulta di computer portatili affidati in uso.

Un bilanciamento degli interessi e dei diritti contrapposti dovrà tenere in debita conside-

I ruoli della Privacy in azienda

I ruoli riconosciuti dalla legge nell'organizzazione della funzione privacy in azienda sono tre, il Titolare, i Responsabili e gli incaricati. Al Titolare compete l'impostazione della gestione della privacy, la predisposizione dell'informativa e della notificazione, le istruzioni a Responsabili e incaricati, l'adozione di idonee misure di sicurezza, il controllo - anche mediante verifiche periodiche - sul rispetto delle disposizioni, della normativa e sulla puntuale osservanza della legge e delle istruzioni impartite. Oltre a ciò il Titolare deve prevedere programmi di formazione continua degli incaricati.

La notificazione, prevista agli art. 37 e 38 del Codice Privacy, è una comunicazione importante al Garante che va effettuata in casi particolari, prima dell'inizio del trattamento e anteriormente alla variazione o cessazione del trattamento. Questo adempimento, che prevede una sanzione amministrativa per omessa/incompleta notificazione (art. 163) e una sanzione penale per infedele notificazione (art.168), va fatto soltanto se l'azienda si avvale di particolari trattamenti che il Garante giudica particolarmente delicati nelle loro conseguenze. Tra questi i più frequenti sono:

- trattamenti elettronici a fine di profilazione clientela;
- banche dati a fine di selezione personale conto terzi (contenenti dati sensibili);
- banche dati relative al rischio di solvibilità economica/patrimoniale, a comportamenti illeciti/fraudolenti.

I Responsabili, indicati all'art. 29, sono a nomina facoltativa e devono essere scelti con requisiti di esperienza, capacità, affidabilità ed effettivo potere: non sono ammessi prestanomi. Devono ricevere un'indicazione scritta dei loro compiti e riferire periodicamente sull'attività al Titolare. Il loro elenco, sempre aggiornato, deve essere disponibile al pubblico, per esempio, sul sito internet dell'impresa. Quando un trattamento si avvale di *outsourcer*, dei quali non si può controllare l'organizzazione, costoro vengono definiti autonomi Titolari di trattamento: quando si tratti di società collegate spesso si usa invece la figura di Responsabile esterno. In entrambi i casi i ruoli sono definiti per iscritto da opportune nomine.

Gli incaricati infine sono persone fisiche, cioè i dipendenti, che operano sotto la diretta autorità del Titolare o del Responsabile; devono essere nominati per iscritto con individuazione dell'ambito di trattamento consentito; devono attenersi alle istruzioni ricevute da Titolare e/o dal Responsabile; hanno necessità di formazione, in particolare devono ricevere specifiche istruzioni per una serie di misure minime di sicurezza nel trattamento, tra cui l'adozione delle necessarie cautele per assicurare la segretezza della parola chiave per non lasciare incustodito ed accessibile lo strumento elettronico durante una sessione di lavoro, per garantire il salvataggio dei dati con frequenza almeno settimanale, per la corretta custodia ed uso dei supporti rimovibili (per dati sensibili e giudiziari), per controllare e custodire gli atti e documenti cartacei contenenti dati personali.

Di particolare rilievo è la separazione di responsabilità tra Titolare e incaricati ai fini di eventuali sanzioni anche penali previste dalla legge. Se il Titolare omette di dare istruzioni su casi specifici e l'incaricato sbaglia, non può essere reso responsabile di ciò: il Titolare ha il compito di prevedere e sorvegliare la gestione della privacy nella sua azienda. Se viceversa l'incaricato, che abbia ricevuto adeguata formazione, si comporta in aperta violazione delle istruzioni ricevute, di ciò può essere reso lui stesso responsabile in riferimento alle norme che regolano il rapporto di lavoro.

razione i principi generali sopra esposti, soprattutto quelli di necessità, pertinenza e non eccedenza.

Per quanto attiene le misure di sicurezza, al fine di ridurre al minimo i rischi di perdita dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alla finalità della raccolta prevede, l'art. 31 prevede l'adozione di idonee misure di sicurezza in relazione al progresso tecnologico, alla natura dei dati ed alle specifiche caratteristiche del trattamento. Ciò implica non solo una mera e statica adozione delle misure minime imposte dall'art. 34 e all'allegato B del Codice[10], ma l'identificazione e l'aggiornamento costante dei processi riguardanti il controllo della sicurezza fisica (dal controllo dell'accesso ai locali alla custodia dei supporti magnetici), logica (protezione delle informazioni e dei sistemi da danni legati a malfunzionamenti tecnologici accidentali o volontari[11]) e organizzativa (gestione della sicurezza, *policy*, linee guida e procedure, audit[12]) al fine di garantire la riservatezza, integrità e disponibilità delle informazioni. Se da un lato l'analisi dei rischi, prevista dal *Documento Programmatico sulla Sicurezza*, appare un utile momento per l'identificazione delle misure idonee di sicurezza, ivi incluse quelle informatiche, appaiono opportune l'identificazione di procedure ed istruzioni operative, il

[10] Come autenticazione informatica, procedure di gestione delle credenziali di autenticazione, sistema di autorizzazione e gestione dell'ambito di trattamento consentito ai singoli incaricati, protezione da accessi non consentiti, procedure per custodia dei backup e ripristino dei sistemi, tenuta ed aggiornamento del documento programmatico della sicurezza.

[11] Per esempio, credenziali di autenticazione informatica individuali da modificarsi periodicamente, adozione ed aggiornamento antivirus, predisposizione e controllo di *firewall*.

[12] Come distribuzione compiti ed assegnazione incarichi, formazione e sensibilizzazione alle problematiche della sicurezza a tutto il personale, o piano di *disaster recovery*.

monitoraggio dei processi aziendali anche attraverso costanti verifiche interne tecnico-organizzative e audit, come previsto dalle norme internazionali ISO 9001, riguardanti la qualità, o più specificatamente dalle norme ISO/IEC 27001, riguardanti i Sistemi di Gestione della Sicurezza delle informazioni.

La previsione dell'autenticazione informatica prefigura anche l'impiego delle tecnologie biometriche che consentono di verificare l'identità di un soggetto attraverso l'impronta digitale, l'iride, il timbro vocale e perfino i tratti somatici del volto. Tale utilizzo deve essere effettuato nel rispetto dei citati principi di finalità, necessità e proporzionalità tanto da rendere non consentito l'utilizzo generalizzato ed indiscriminato dei dati biometrici solamente se giustificato da una generica esigenza di sicurezza[13].

Per quanto attiene alla problematica delle etichette RFID (*Radio Frequency Identification*) con tale termine si fa riferimento ai dispositivi basati sull'identificazione attraverso radiofrequenze, rientranti nell'ampia categoria delle tecnologie di identificazione automatica che include anche i lettori ottici di caratteri (OCR), i lettori di codici a barre (*barcode*) ed alcune tecnologie biometriche. Finora le etichette RFID sono state usate soprattutto per l'identificazione e la gestione di prodotti, per il controllo della catena distributiva o per tutelare l'autenticità di singoli marchi; tuttavia, potrebbero essere messe in relazione con dati personali (come quelli ricavabili dalle carte di credito) e potrebbero essere utilizzate perfino per raccogliere informazioni oppure per localizzare o classificare individui in possesso di oggetti che rechino tali etichette. La tecnologia in questione consentirebbe di ricostruire le attività di singoli individui e di profilare o tracciare i percorsi effettuati dagli stessi, controllarne la posizione geografica o verificare quali prodotti usa, indossa, trasporta.

I rischi possono, inoltre, accrescersi nel caso di interazione delle tecnologie RFID con infrastrutture di rete, come la telefonia e internet, consentendo una lettura delle etichette a distanze sempre maggiori. Per queste ragioni il Garante ha emanato un provvedimento generale sottolineando la necessità di rispettare tutti i principi fondamentali della normativa in materia di privacy sia nella realizzazione che nell'utilizzazione dei dispositivi RFID e in particolare:

a. prima di ricorrere a etichette RFID connesse a dati personali, o tali da consentire la classificazione in base a profili della clientela, ciascun Titolare di trattamento dovrebbe valutare approcci alternativi che consentano di raggiungere lo stesso obiettivo;

b. qualora il Titolare del trattamento dimostri che è indispensabile ricorrere a dati personali, questi ultimi devono essere raccolti in modo chiaro e trasparente;

c. i dati personali possono essere utilizzati esclusivamente per lo scopo specifico per cui sono stati inizialmente raccolti e possono essere conservati soltanto finché risultino necessari al raggiungimento (o al soddisfacimento) di tale scopo;

d. i singoli interessati dovrebbero avere la possibilità di cancellare i dati e di disattivare o distruggere le etichette RFID una volta che ne siano entrati in possesso.

A detta dell'*Authority* è sempre necessario informare dell'utilizzo di questi sistemi, nonché dell'esistenza dei lettori che attivano l'etichetta (va apposta un'informativa anche sui prodotti che recano le etichette); deve essere, inoltre, garantito il diritto di asportare o disattivare in modo agevole il funzionamento delle RFID al momento dell'acquisto del prodotto (le etichette devono essere facilmente asportabili senza danneggiare o limitare la funzionalità del prodotto, per esempio, collocandole solo sulla confezione).

Oltre a questi argomenti e alla problematiche connesse, l'attenzione del Garante italiano, così come in altri paesi europei, si è rivolta al delicato bilanciamento tra tutela dei dati per-

[13] Il provvedimento del Garante del 27 ottobre 2007, pur acconsentendo agli Istituti Bancari di utilizzare per esempio la rilevazione delle impronte digitali in combinazione con le immagini raccolte attraverso la videosorveglianza, impone precise misure, accorgimenti ed adempimenti al fine del bilanciamento di interesse tra esigenza di sicurezza specifica e tutela degli interessati (specifica notifica al Garante con documentazione di rischio concreto dello sportello bancario, tempo massimo di conservazione delle informazioni ed utilizzo della crittografia, possibilità alternative di accesso alla banca, opportuna e visibile informativa ecc.).

sonali e sicurezza dei cittadini e lotta al terrorismo. Il nuovo presidente prof. Francesco Pizzetti ha lanciato un allarme proprio su queste transazioni, sottolineando l'illegittimità del trasferimento di dati personali negli Stati Uniti imposto dalle transazioni bancarie internazionali per esempio sul circuito Swift. La lotta al terrorismo internazionale imposta dagli Stati Uniti dopo i tragici fatti dell'11 settembre ha richiesto alcuni sacrifici sul fronte della tutela dei dati personali: per essere autorizzate ad atterrare negli USA le compagnie aeree europee debbono fornire, senza le opportune tutele, una serie di dati personali dei passeggeri che vanno ben oltre lo scopo dichiarato, trasformando ogni soggetto in un potenziale indagato: anche su questo tema i Garanti europei si sono espressi unanimemente a più riprese in maniera contraria, manifestando una forte preoccupazione per questa schedatura dei cittadini dell'Unione, che è arrivata all'attenzione della Commissione Europea.

I temi più caldi di cui certamente si dibatterà in futuro e che porteranno probabilmente a cambiamenti nella normativa, non solo in Italia ma su scala almeno europea, saranno:

- la diversità di ampiezza della tutela dei dati personali tra Europa e Stati Uniti;
- come conseguenza di ciò, la lotta allo *spamming* (comunicazioni elettroniche non sollecitate) che negli Stati Uniti non è punito allo stesso modo che in Europa[14];
- l'equilibrio tra diritto alla riservatezza e diritto di cronaca, con particolare riguardo alla libertà di stampa;
- la regolamentazione della cancellazione dei dati trascorso un certo periodo di tempo (si pensi ai dati sul web) e bilanciamento delle esigenze tra diritto all'oblio e storia.

Le sanzioni

Sanzioni amministrative

- Omessa o inidonea informativa all'interessato
pagamento somma da 3.000 a 18.000 € (da 5.000 a 30.000 € se si tratta di dati sensibili) aumentabile fino al triplo
- mancata o incompleta notificazione
pagamento somma da 10.000 a 60.000 €
- omessa informazione o esibizione al Garante
pagamento somma da 4.000 a 24.000 €

Sanzioni penali

- Trattamento illecito di dati
reclusione da 6 a 18 mesi (da 6 a 24 mesi se consiste in comunicazione o diffusione, ovvero da 1 a 3 anni se dal fatto deriva nocumento)
- falsità nelle dichiarazioni e notificazioni al Garante
reclusione da 6 mesi a 3 anni
- omissione delle misure minime di sicurezza
arresto fino a 2 anni o ammenda da 10.000 a 50.000 €
- inosservanza di provvedimenti del Garante
reclusione da 3 mesi a 2 anni

4. Sanzioni e responsabilità

In caso di violazione delle norme in materia di protezione dei dati personali sono previste sanzioni amministrative e penali [riquadro]. Le prime rientrano nella competenza del Garante, secondo la procedura delineata nel Codice e integrata dalla legge 24 novembre 1981 n. 689 (legge sulle sanzioni amministrative). Il Titolare, entro 60 giorni dalla contestazione, può far pervenire le proprie difese, allegando eventuali documenti e richiedendo di essere sentito personalmente. Esaurita la fase istruttoria, l'Autorità, qualora ritenga accertata la violazione, commina la sanzione e ne ingiunge il pagamento con un ordinanza motivata. Il Titolare, nel termine di 30 giorni dalla notifica del provvedimento, può versare quanto dovuto oppure presentare opposizione all'ordinanza-ingiunzione davanti al giudice. Se la violazione è compiuta da più soggetti (per esempio nel caso di co-titolari del medesimo trattamento), viene irrogata una sanzione per ciascuno; al contrario, se l'illecito è imputato a un dipendente è prevista la responsabilità solidale del datore di lavoro (ciò significa che la sanzione sarà unica e il Titolare potrà eventualmente rivalersi nei confronti dell'autore dell'illecito, come previsto dalle norme del diritto civile e del lavoro).

Le sanzioni penali, invece, possono essere irrogate soltanto da un giudice, in caso di pronuncia di condanna, all'esito di un processo che verifichi in concreto la sussistenza del reato e ne ascriva la responsabilità all'imputato. Il Titolare del trattamento[15], visto il suo ruolo

[14] Non è un caso che la valanga di spam che si riceve ogni giorno provenga dagli Stati Uniti o da altri Paesi privi di tutela giuridica equivalente a quella Europea. Chi effettua spam a partire dall'Italia rischia pene severe proprio ai sensi del Codice Privacy.

[15] E anche il Responsabile, se nominato.

chiave in tutta la normativa sulla privacy, risulta il principale indagato. L'ipotesi delittuosa principale è quella di trattamento illecito di dati personali che prevede la violazione di precetti molto eterogenei che spaziano dalle norme sul consenso al trattamento alle regole in tema di comunicazioni indesiderate, con particolare inasprimento delle pene previste per la comunicazione e la diffusione dei dati sensibili.
In caso di trattamenti illeciti, a prescindere dalle sanzioni amministrative e penali, può configurarsi una responsabilità civile, vale a dire l'obbligo di risarcire il danno prodotto. A norma del Codice della privacy, infatti, chiunque subisce un danno per effetto del trattamento di dati personali ha diritto al risarcimento, salvo che il Titolare dimostri di aver adottato tutte le misure idonee a evitarlo: in buona sostanza il danneggiato può limitarsi a dimostrare di aver subito un danno a causa del trattamento, mentre il danneggiante, per sottrarsi alla condanna, deve provare al giudice di aver osservato tutte le norme previste dalla legge, dettate dal Garante e suggerite dalla diligenza. In realtà questa prova si rivela estremamente difficile da fornire in giudizio, per la semplice considerazione che l'illecito che causa il danno è sempre frutto di una lacuna del Titolare, salvi rari casi fortuiti o di forza maggiore (la situazione è simile a quella dell'automobilista che, rispettando alla perfezione il codice della strada, non causerebbe alcun sinistro mentre, al contrario, ogni incidente deriva dalla violazione di una norma o di una regola di prudenza). Ovviamente, secondo gli ordinari principi della responsabilità civile, il datore di lavoro è tenuto a risarcire il danno arrecato dal suo dipendente nell'esercizio delle proprie mansioni, salvo il diritto di rivalsa e l'irrogazione di eventuali sanzioni disciplinari, in riferimento alle norme che regolano il rapporto di lavoro: un esempio è il caso dell'infermiere che comunichi a un giornale scandalistico i dati sanitari di un paziente famoso; costui presumibilmente richiederà un risarcimento dei danni all'ospedale, che in seguito potrà chiamare in giudizio il dipendente.
I principi esposti sono da ritenersi pienamente vigenti anche rispetto alle attività di trattamento della Pubblica Amministrazione, non potendo essere contraddetti né dalla presunzione di legittimità dell'azione amministrativa, né dalla discrezionalità a essa riferibile (suscettibile sempre di valutazione da parte del giudice) o ancora dall'utilità sociale del suo agire.
Per quanto concerne la valutazione del risarcimento, il Codice dispone che venga liquidato non solo il danno patrimoniale, ma anche quello non patrimoniale (per esempio il danno morale e biologico), e consente al giudice, qualora non risulti comprovato l'ammontare preciso del danno patito, di utilizzare anche criteri di valutazione equitativa, che soppesino la gravità del fatto. Molto spesso inoltre la tutela predisposta dal Codice della privacy si affianca a quella garantita da altre norme: per esempio in relazione alla foto di una persona, oltre alle norme sulla riservatezza si può richiamare la tutela della fotografia (e i diritti di sfruttamento) stabilita dalla legge sul diritto d'autore; oppure la pubblicazione di certe informazioni, al di là della privacy, può sostanziarsi in una lesione della dignità o dell'immagine professionale di un soggetto (ovvero commerciale se trattasi di un'impresa).
I tribunali italiani, con sentenze pronunciate già in applicazione della precedente legge 675/96, hanno emesso condanne piuttosto pesanti in termini economici; il caso certamente più noto alle cronache vede protagonista un istituto bancario che nel corso dell'istruzione di una pratica di mutuo a favore di due coniugi viene citato in giudizio dagli stessi per trattamento illecito dei dati personali. La banca aveva, infatti, diffuso informazioni confidenziali sui propri clienti lasciando incustodita nell'atrio il fascicolo di richiesta di mutuo contenente apprezzamenti poco lusinghieri sulla loro vita personale e coniugale (di ciò gli interessati erano venuti a conoscenza casualmente). Il Tribunale di Orvieto ha ravvisato nel comportamento illegittimo della banca una lesione della dignità personale, professionale e commerciale degli interessati, sostenendo che il trattamento illecito dei dati personali può produrre un danno non patrimoniale di cui è possibile chiedere il risarcimento in sede giudiziaria indipendentemente dall'esistenza di un danno di natura patrimoniale. In accoglimento della domanda dei due coniugi, il giudice ha condannato l'istituto di credito al pagamento in via equitativa di 25.000 euro in favore di ambedue i coniugi. Si contano infine numerose pure

le pronunce relative a trattamenti senza il consenso dell'interessato e, in particolare, alla pubblicazione su giornali di dati personali che eccedono il diritto di cronaca.

5. Conclusione

Dieci anni di privacy in Italia, in conclusione, hanno fatto compiere al nostro Paese una lunga strada, ma ancora tanta deve essere percorsa, purtroppo talora anche nel convincere taluni che l'argomento va preso con serietà e non denigrato e minimizzato come insignificante. Su questo punto è necessario da parte di tutti, Autorità Garante, aziende e semplici cittadini, una fermezza estrema: chi ritiene che la tutela dei dati personali sia un inutile sofisma, non conosce o sottovaluta gravemente le possibilità di conservazione e aggregazione dell'informazione offerte dalle tecnologie odierne.
La tutela dei dati personali è una normativa che ha per oggetto il rispetto dell'individuo, nella sua forma più ampia e la difesa della libertà di ciascun cittadino a tutto tondo: la storia di ogni tempo dimostra che un paese in cui sia tollerato di derogare o irridere questi temi si avvia inevitabilmente su una strada pericolosa, amara e senza ritorno.

Leonardo Felician, laureato in Fisica alla Scuola Normale Superiore di Pisa, insegna *Sistemi Informativi II* nel corso di laurea in Ingegneria Informatica dell'Università di Trieste e *Economia delle Imprese di Assicurazioni II* presso la facoltà di Economia e Commercio dell'Università di Pisa. Direttore generale di imprese assicurative, si è cimentato a lungo e in prima persona in ambito accademico e aziendale su temi inerenti la *privacy*.
E-mail: lfelician@units.it

Antonio Piva, laureato in Scienze dell'Informazione, *Vice Presidente dell'ALSI* (Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica) e Presidente della commissione di informatica giuridica. Docente a contratto di *diritto dell'ICT e qualità* all'Università di Udine. Consulente sistemi informatici e Governo Elettronico nella PA locale, valutatore di sistemi di qualità ISO9000 ed ispettore AICA.
E-mail: antonio@piva.mobi

David D'Agostini avvocato, master in informatica giuridica e diritto delle nuove tecnologie, collabora all'attività di ricerca scientifica dell'Università degli studi di Udine e ha fondato l'associazione "*Centro Innovazione & Diritto*". È componente della Commissione Informatica dei Consigli dell'Ordine del Triveneto, responsabile dell'area "*Diritto & informatica*" della rivista "*Il foro friulano*", membro dell'organo di Audit Interno di Autovie Venete SpA.
E-mail: studio@avvocatodagostini.it