CONSIGLIO NAZIONALE
DEI DOTTORI COMMERCIALISTI

FONDAZIONE
ARISTEIA
ISTITUTO DI RICERCA
DEI DOTTORI
COMMERCIALISTI

DOCUMENTI ARISTEIA

documento n. 3

Misure di sicurezza per la protezione dei dati personali negli studi professionali

maggio 2001

MISURE DI SICUREZZA PER LA PROTEZIONE DEI DATI PERSONALI NEGLI STUDI PROFESSIONALI

DOCUMENTO ARISTEIA N. 3

MISURE DI SICUREZZA PER LA PROTEZIONE DEI DATI PERSONALI NEGLI STUDI PROFESSIONALI

(artt. 15, 18 e 36 della Legge 31 dicembre 1996 n. 675 *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e successive modificazioni ed integrazioni*; DPR 28 luglio 1999 n. 318 *Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675*; Legge 3 novembre 2000 n. 325 *Disposizioni inerenti all'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste dall'articolo 15 della legge 31 dicembre 1996 n. 675*)

SOMMARIO: 1. Scopo del documento e breve inquadramento sistematico della normativa sulla privacy - 2. Obblighi gravanti sul titolare del trattamento e diversi dalle misure di sicurezza. Cenni - 3. La nozione di sicurezza nel trattamento dei dati personali: misure di sicurezza "idonee" e "minime" - 4. Termini temporali di adozione delle misure di sicurezza - 5. Il regime sanzionatorio inerente le misure di sicurezza. Cenni - 6. Indicazioni specifiche sulle misure di sicurezza adottabili negli studi professionali - 7. Precisazioni conclusive sul documento programmatico sulla sicurezza

1. SCOPO DEL DOCUMENTO E BREVE INQUADRAMENTO SISTEMATICO DELLA NORMATIVA SULLA PRIVACY

Il presente documento intende fornire, nei limiti dei riferimenti normativi, giurisprudenziali e dottrinali attualmente disponibili, alcune indicazioni di carattere interpretativo ed applicativo sulle "misure di sicurezza" richieste dalla vigente normativa in materia di tutela della riservatezza dei dati personali o "privacy", ponendo particolare attenzione alle problematiche degli studi professionali.

L'esigenza di una nuova riflessione sulla privacy discende sia dall'esaurimento dei tempi accordati dal legislatore per adeguarsi completamente alle norme, sia dalle recentissime segnalazioni del Garante, il quale denuncia diffuse irregolarità nel trattamento di dati riservati.

La disciplina della privacy è stata introdotta in Italia con la L. n. 675/96, entrata in vigore l'8 maggio del 1997, la quale appresta piena attuazione alle prescrizioni contenute nella "Convenzione di Strasburgo" del 28 gennaio 1981, nel Trattato di Schengen del 1985 e nella Dir. 95/46/CE del

Parlamento Europeo e del Consiglio del 24 ottobre 1995. Il quadro normativo delineato dalle menzionate fonti ascrive il diritto alla riservatezza nel novero dei diritti fondamentali della persona, qualificandolo però in modo relativo ed elastico: pertanto, la privacy significa diritto della persona, fisica o meno, non all'assoluto isolamento, bensì alla conoscenza, al controllo e – se del caso – alla modificazione delle informazioni sul proprio conto trattate da altri soggetti (cd. "autodeterminazione informativa").

Inoltre, la disciplina legale della privacy, lungi dall'essere generalizzata per tutte le informazioni riferibili ad un soggetto, risulta graduale e differenziata sulla base di criteri diversi, quali:

- la criticità del dato (si distingue tra: dati pubblici o conoscibili da chiunque; dati concernenti lo svolgimento dell'attività economica; dati personali non sensibili; dati sensibili in genere; dati sensibili sanitari, sessuali e giudiziari);
- la natura del soggetto nel cui interesse le informazioni sono trattate o "titolare del trattamento", che può appartenere alla categoria dei soggetti privati ed enti pubblici economici, dei soggetti pubblici non economici, dei liberi professionisti, dei professionisti medici o dei giornalisti;
- la natura del soggetto cui le informazioni si riferiscono o "interessato", che può essere persona fisica o persona non fisica;
- le finalità del trattamento, il quale può essere svolto per fini esclusivamente personali, per ragioni di giustizia o per fini diversi dai precedenti;
- la natura del trattamento, che può essere automatizzata o con elaboratori elettronici oppure manuale;
- il tipo di operazione (trattamento in genere, raccolta diretta – presso l'interessato – o indiretta, comunicazione, diffusione, trasferimento all'estero di dati).

2. Obblighi gravanti sul titolare del trattamento diversi dalle misure di sicurezza. Cenni

Oltre alle misure di sicurezza, il legislatore richiede agli operatori una serie di cautele ed adempimenti. In estrema sintesi, oltre all'adozione delle misure di sicurezza, al titolare del trattamento è fatto obbligo di:

- fornire all'interessato – prima della raccolta dei dati presso lo stesso - adeguata informativa sul trattamento che si intende effettuare (cd. raccolta diretta);

- fornire, anteriormente alla registrazione o comunque alla prima comunicazione dei dati, apposita informativa all'interessato sul trattamento che si intende effettuare con i dati raccolti su di lui presso terzi diversi dall'interessato medesimo (cd. raccolta indiretta);
- chiedere ed ottenere dall'interessato il consenso espresso (ossia anche mediante verbalizzazione o delibera formale, nel caso di P.A. e grandi organizzazioni) per i dati personali e scritto per quelli sensibili;
- chiedere all'Autorità Garante per la protezione per i dati personali l'autorizzazione al trattamento dei dati sensibili;
- notificare al Garante informazioni su fini, tempi, modi e contenuti dei trattamenti (cd. notificazione generale);
- notificare al Garante la cessazione del trattamento;
- fare apposita notificazione al Garante per il trasferimento all'estero dei dati (cd. notificazione speciale);
- designare l'incaricato/i del trattamento dei dati, con la cautela per cui l'incaricato deve essere necessariamente persona fisica;
- limitatamente ai titolari aventi natura di soggetto pubblico non economico, osservare il principio per cui il trattamento di dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla legge e dai regolamenti, con obbligo di preventiva comunicazione al Garante qualora si intenda procedere alla comunicazione o diffusione di dati ad altri soggetti pubblici non economici in assenza di espresse norme che lo consentano.

Tuttavia, al fine di raggiungere un adeguato bilanciamento tra il diritto alla riservatezza ed altri diritti, il regime sommariamente indicato non si applica integralmente a tutti gli operatori ed a tutti i trattamenti. Infatti, in considerazione dei molteplici fattori alla base della disciplina della privacy, nella legge figurano molteplici esoneri ed esenzioni.

In particolare, la categoria dei liberi professionisti beneficia di un regime normativo più favorevole e tenue, poiché la preesistente regolamentazione professionale e le emanazioni di autodisciplina da parte degli Ordini di appartenenza costituiscono condizioni favorevoli a comportamenti corretti e consoni anche in fatto di trattamento delle informazioni altrui. Nondimeno, la legge ed il Garante – nel prevedere riferimenti normativi e provvedimenti sulla privacy specificamente rivolti ai professionisti – sottolineano l'importanza del tema per la categoria, essendo quella professionale un'attività che tipicamente si sostanzia della raccolta, elaborazione e divulgazione di informazioni.

Ad ogni modo, l'interpretazione letterale e sistematica della normativa in esame consente di sostenere che il professionista, nello svolgimento della propria attività, non è tenuto a:

- raccogliere il consenso espresso per il trattamento dei dati personali non sensibili;
- effettuare la notificazione generale al Garante;
- effettuare la notificazione né di cessazione né speciale, quando il soggetto cui i dati si riferiscono sia persona non fisica (quindi, per la clientela aziendale, gli enti locali e gli altri enti territoriali ed istituzionali), in base all'art. 26 c. I l. n. 675/96;
- richiedere individualmente al Garante l'autorizzazione al trattamento dei dati sensibili, dovendosi attenere all'autorizzazione generale o di categoria n. 4 (per i rapporti con clienti e fornitori) ed a quella n. 1 e n. 2, rispettivamente, per i dati relativi a collaboratori e dipendenti e quelli sanitari.

Incerti restano tuttora altri profili, tra i quali la sussistenza o meno in capo al dottore commercialista dell'obbligo della notificazione di cessazione del trattamento e/o di quella cd. speciale per i dati relativi a persone fisiche (contribuenti, liberi professionisti e piccoli imprenditori). La dottrina propende per la soluzione affermativa nel secondo caso, mentre sul primo mancano argomentazioni altrettanto convincenti: ad ogni conto, l'obbligo di notificazione di trasferimenti all'estero di dati non sarebbe particolarmente gravoso, atteso che l'operazione in sé risulta praticamente marginale per la prevalenza degli studi professionali; diversamente, l'obbligo di notificazione di cessazione di alcuni trattamenti potrebbe cogliere alcuni studi in una situazione di non piena regolarità – qualora ci siano state cessazioni dall'8 maggio 1997 ad oggi – ma il problema sarebbe superato quando si accolga la tesi della dottrina, secondo cui questo tipo di notificazione può essere anche successivo alla cessazione.

Inoltre, non è ben chiaro se per la conservazione dei dati cd. storici o pregressi - ai fini di consultazione personale e di formazione di una sorta di "prassi del professionista" – sia possibile invocare alcune norme della legge, nella fattispecie l'art. 3 c. I L. n. 675/96. La soluzione negativa imporrebbe la distruzione degli archivi oppure la trasformazione in forma anonima di tutti i dati, mediante l'eliminazione dei riferimenti che consentono la riconduzione dei dati – specie se sensibili – all'interessato.

Infine, dovrebbe essere corretta l'interpretazione secondo cui al dottore commercialista che operi a tutela dell'interesse pubblico nell'ambito di vicende giudiziarie – come nell'ambito delle procedure concorsuali – non si applichi la normativa sulla privacy, ai sensi della deroga di cui all'art. 4 c. I lett.

d) L. n. 675/96, fatta salva la vigenza di specifiche disposizioni (tra le quali rientrano quelle sulle misure di sicurezza) che assicurano la liceità della gestione dei dati.

3. LA NOZIONE DI SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI: MISURE DI SICUREZZA "IDONEE" E "MINIME"

L'art. 15 L. n. 675/96 introduce il concetto di misure di sicurezza, ossia le modalità operative con cui devono essere gestiti i dati personali contenuti negli archivi, sia cartacei che elettronici, al fine di proteggere i dati da perdita, distruzione o intrusioni. La norma rappresenta uno dei precetti fondamentali della normativa sulla privacy, insieme agli artt. 1, 9, 13 L. n. 675/96, che enunciano, rispettivamente, le finalità della legge, i requisiti che devono possedere i dati ed i trattamenti e i diritti di tutela che spettano all'interessato.

La funzione complementare ed integrativa della sicurezza dei dati è evidente: mentre l'informativa, il consenso, le notificazioni e le richieste di autorizzazione sono adempimenti imposti al titolare per permettere all'interessato di esercitare i propri diritti e/o trovare ulteriore tutela in provvedimenti preventivi o successivi del Garante, le misure di sicurezza assicurano continuità alle garanzie e cautele che il titolare si è impegnato, al momento della raccolta delle informazioni, a fornire. La sicurezza informativa riveste un'importanza talmente rilevante nella normativa in esame che gli artt. 3 c. II e 4 c. II l. n. 675/96 impongono l'adozione dei provvedimenti atti a perseguirla anche a quei trattamenti sottratti al campo di applicazione della legge sulla privacy.

Lo stesso Garante ha ricordato chiaramente che l'esigenza della sicurezza è coessenziale a qualsiasi tipo di trattamento di dati, essendo un presidio contro il rischio della loro distruzione o perdita, anche accidentale, e contro il pericolo di accessi non autorizzati. L'art. 15 L. n. 675/96 disciplina le misure di sicurezza prevedendo due distinti livelli di protezione dei trattamenti:

- da un lato quello massimo, corrispondente alle cd. misure di sicurezza idonee - non specificate, ma individuabili sulla base delle conoscenze tecniche concretamente disponibili in un dato istante - la violazione delle quali comporta responsabilità civile in caso di danno;
- dall'altro lato quello minimo, rappresentato dalle cd. misure di sicurezza minime, specificamente individuate all'interno di un ulteriore atto (il DPR. n. 318/99) e la violazione delle quali comporta responsabilità civile e penale.

La conferma letterale del peculiare impianto dicotomico e dualistico della norma è fornita dal fatto che tanto delle misure idonee quanto di quelle minime venga precisata la natura preventiva, come se si trattasse di due aspetti affatto disgiunti.

Con riguardo alle misure idonee, l'art. 15 c. I L. n. 675/96 stabilisce un vero e proprio obbligo di sicurezza, inteso come obbligo di custodia e conservazione dei dati: questa qualificazione è espressiva della portata ampia della norma, poiché la nozione di custodia non si esaurisce nella mera conservazione ed il controllo, lungi dall'implicare un accertamento occasionale ed ispettivo, implica un potere effettivo e permanente sul dato. La gravosità dell'obbligo traspare anche dalla definizione relativa fornita dal legislatore, secondo cui le misure di sicurezza:

- sono "preventive";
- devono essere "idonee", ossia adottate "anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento";
- sono finalizzate alla minimizzazione dei "rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

La disposizione appare molto esigente, soprattutto se si considera che il principio di proporzionalità e commisurazione implicito nel requisito di idoneità delle misure di sicurezza non viene specificato in modo esaustivo e non è contemperato dal riferimento ai costi di implementazione, invece presente nella dir. 95/46/CE. In sintesi, secondo il Garante, l'art. 15 c. I L. n. 675/96 richiede al titolare uno sforzo di perseguimento della sicurezza informativa continuo e mai definitivo, imponendogli di ridurre al minimo i predetti rischi mediante l'utilizzazione di sistemi di sicurezza costantemente adeguati nel tempo.

Come anticipato, l'art. 15 c. II-III L. n. 675/96 si distacca nettamente dal contenuto del comma precedente, introducendo le "misure minime di sicurezza", la cui disciplina è rinviata al regolamento approvato con il DPR. n. 318/99 ed agli adeguamenti almeno biennali, "in relazione all'evoluzione tecnica del settore e all'esperienza maturata", dello stesso. Nello specifico, l'art. 1 lett. a DPR. n. 318/99 intende per misure minime "il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, previste nel presente regolamento, che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dall'articolo 15, comma 1, della legge": la definizione risulta coerente anche con l'art. 36 L. n. 675/96, che si riferisce alle misure in esame denominandole "misure necessarie a garantire la sicurezza dei dati personali", quasi a sottolinearne la valenza indispensabile ma non sufficiente.

Come ha chiarito il Garante, il DPR. n. 318/99 – composto da 10 articoli e rivolto a tutti i soggetti, pubblici e privati, che svolgono trattamenti di dati personali – non contiene tutte le regole tecniche da adottare in ogni caso né le migliori misure evidenziate dalla scienza tecnica in un dato momento, bensì individua unicamente quei requisiti minimi il cui mancato rispetto comporta una maggiore esposizione a rischio del bene giuridico che la norma vuole tutelare. Al fine di individuare provvedimenti tecnico-organizzativi tipici e standardizzati, il regolamento mutua l'impostazione della L. n. 675/96, graduando le prescrizioni in base a diversi aspetti, quali:

- le finalità del trattamento (per fini esclusivamente personali, per fini diversi dai precedenti);
- la natura del trattamento (automatizzato o con elaboratori elettronici, manuale);
- la tipologia del sistema informativo ove risiedono i dati (non in rete, in rete non disponibile al pubblico, in rete disponibile al pubblico);
- il tipo di dato personale (dati personali non sensibili, dati sensibili o giudiziari).

Con riguardo al primo fattore, il DPR. n. 318/99 accorda un regime più blando ai trattamenti "per fini esclusivamente personali" ex art. 3 l. n. 675/96, in ragione del minore rischio intrinseco. Tuttavia, qualora il trattamento del suddetto tipo coinvolga dati sensibili e giudiziari e sia svolto con "elaboratori stabilmente accessibili da altri elaboratori", l'art. 8 DPR. n. 318/99 impone di "proteggere l'accesso ai dati o al sistema mediante l'utilizzo di una parola chiave, qualora i dati siano organizzati in banche di dati".

Per tutti gli altri tipi di trattamento, le misure minime sono graduate a partire dalla distinzione in base alle modalità di effettuazione delle operazioni: in caso di trattamenti non automatizzati e svolti con l'ausilio di supporti cartacei, l'art. 9 c. I lett. a DPR. n. 318/99 richiede che il titolare o, se nominato, il responsabile autorizzi, nel designare per iscritto gli incaricati del trattamento e nell'impartire le istruzioni, i soggetti abilitati ad accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati, mentre l'art. 9 c. I lett. b DPR. n. 318/99 impone che gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato, nonché conservati e restituiti al termine delle operazioni dagli incaricati cui siano stati affidati. Però, se il trattamento coinvolge dati sensibili o giudiziari, l'art. 9 c. II lett. a DPR. n. 318/99 prevede che:

- gli incaricati conservino in contenitori muniti di serratura, sino alla restituzione, gli atti e documenti concernenti i dati loro affidati;
- l'accesso agli archivi sia controllato e siano identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi;

- con le stesse modalità indicate siano conservati e protetti anche i supporti cartacei contenenti la riproduzione di dati sensibili e giudiziari.

Per quanto concerne i trattamenti condotti, anche in parte, mediante strumenti elettronici o automatizzati, la disciplina risulta ancora differenziata in funzione del tipo di sistema informativo, distinguendosi fra trattamenti di dati personali effettuati mediante elaboratori:

- non accessibili da altri elaboratori o terminali (art. 2 DPR. n. 318/99);
- accessibili in rete (artt. 3 e 7 DPR. n. 318/99), a loro volta articolati in elaboratori accessibili:
  - da altri elaboratori solo tramite reti non disponibili al pubblico (art. 3 c. 1 lett. a DPR. n. 318/99),
  - mediante una rete di telecomunicazioni disponibili al pubblico (art. 3 c. 1 lett. b DPR. n. 318/99).

In questo ambito, assume primario rilievo la distinzione tra "amministratori di sistema" (art. 1 lett. c DPR. n. 318/99), custodi delle parole chiave (arg. art. 2 lett. b DPR. n. 318/99), utenti (art. 4 lett. a DPR. n. 318/99) ed "incaricati della manutenzione" (art. 5 DPR. n. 318/99), nonché il regime di autorizzazioni interne scritte che deve regolare tali qualifiche. Infatti, sebbene – come nota il Garante - il Governo abbia preferito non indicare per ogni singola misura di sicurezza i soggetti tenuti ad adottarla (poiché tale scelta muta a seconda delle attribuzioni e dei ruoli stabiliti all'interno di ciascuna struttura), il fondamento delle indicazioni contenute nel regolamento, soprattutto per i trattamenti automatizzati in rete, giace sull'intersezione di due elementi:

- la valutazione del rischio di perdita, distruzione o accesso abusivo associato al trattamento;
- l'osservanza del principio del "need to know" nell'abilitazione degli incaricati a compiere le diverse operazioni del trattamento, per cui ciascun soggetto deve concretamente impiegare i dati che sono strettamente pertinenti ed utili allo svolgimento del proprio compito.

Attraverso questa interrelazione, il regolamento intende indurre gli operatori a non limitarsi all'adozione di atti formali – come le designazioni, il documento programmatico sulla sicurezza e altri documenti volontari – cui non corrispondano concrete soluzioni organizzative.

4. TERMINI PER L'ADOZIONE DELLE MISURE DI SICUREZZA

In base all'art. 41 c. III l. n. 675/96, le misure minime dovevano essere adottate entro il 29/03/2000 e senza alcun coinvolgimento del Garante, nel senso che, come la stessa Autorità ha chiarito, gli atti

previsti dal regolamento – tra cui il documento programmatico sulla sicurezza o la designazione dei responsabili e degli incaricati del trattamento - e le altre determinazioni imposte dal DPR. n. 318/99:

- non devono essere comunicati al Garante in occasione della loro adozione, bensì esibiti a seguito di un'eventuale e specifica richiesta in sede di ispezione o di controllo da parte dell'Autorità;
- non comportano per i titolari dei trattamenti la modificazione delle notificazioni precedentemente presentate.

Tuttavia, in sede di prima applicazione della legge ed in ragione del generale ritardo degli operatori nell'adeguamento, il legislatore ha emanato la L. n. 325/2000 (cd. legge proroga sulle misure di sicurezza), la quale consentiva ad uffici pubblici, imprese private e liberi professionisti, che non avessero adottato le previste misure minime di sicurezza entro la predetta scadenza, di beneficiare – ai soli fini della responsabilità penale - di un differimento sino al 31/12/2000. Pertanto, la proroga non produce effetti diretti sulla responsabilità civile, che può essere riconosciuta per l'eventuale danno derivato da una mancata o non idonea adozione delle misure di sicurezza a partire dal 29/03/2000.

Per avvalersi della proroga, il titolare – ai sensi dell'art. 1 c. II-III L. n. 325/2000 – doveva predisporre "entro un mese dalla data di entrata in vigore della presente legge" (cioè entro l'11/12/2000) un documento "avente data certa" e contenente "una esposizione sintetica" delle esigenze tecnico-organizzative che hanno reso necessario avvalersi del differimento dei termini, comprensiva dell'articolazione del programma di adeguamento - con indicazione delle scelte già adottate e da adottare - e delle "linee-guida previste per dare piena attuazione alle misure minime di sicurezza […] nonché alle più ampie misure di sicurezza previste dal comma 1 dell'articolo 15 della medesima legge n. 675 del 1996", conservandolo presso di sé ai fini, evidentemente, probatori. Il Garante, in sede di esplicazione della norma, ha chiarito il requisito formale della "data certa" richiamando la disciplina civilistica in materia di prove documentali (artt. 2702-2704 cod. civ.) e suggerendo alcune modalità di adempimento.

Il riferimento della L. n. 325/2000 alle misure sia minime sia idonee ha suscitato perplessità ad una prima lettura, ma è invero corretto e coerente: infatti, il dilazionamento dei tempi di implementazione delle misure minime di sicurezza non poteva non interessare anche i termini sulle misure idonee, poiché altrimenti si sarebbe incorso nel paradosso per cui il livello di protezione minimo potesse essere assicurato successivamente a quello massimo. Per questa ragione, già l'art. 41 c. III ult. pt. L. n. 675/96 prevede che, fino al decorso del termine relativo alle misure minime, "i dati personali devono essere custoditi in maniera tale da evitare un incremento dei rischi di cui all'articolo 15, comma 1".

Quindi, è evidente che, fissato al 31/12/2000 il termine massimo di adozione delle misure minime, a partire da tale data vanno anche implementate le misure idonee. In tal senso, il richiamo della L. n. 325/2000 alle "linee-guida" non deve essere equivocato, riguardando quello il documento che doveva essere elaborato per beneficiare della proroga e non la scadenza del 31/12/2000, a partire dalla quale tutte le misure di sicurezza devono risultare operative e l'art. 15 L. n. 675/96 diventa pienamente vigente, sul versante tanto penale quanto civile.

5. IL REGIME SANZIONATORIO INERENTE LE MISURE DI SICUREZZA. CENNI

Il punto fondamentale che merita di essere evidenziato ai fini della corretta interpretazione del concetto di misure di sicurezza è che tutte le misure, minime o idonee, partecipano - per espresso riferimento della L. n. 675/96 – al controllo del rischio di danno per mezzo di un costante aggiornamento verso la migliore tecnica, per cui il processo di applicazione delle norme non può mai essere considerato, neppure per le misure in qualche modo "standardizzabili", definitivo e concluso. Per questo motivo, all'art. 15 L. n. 675/96 corrisponde un sistema sanzionatorio assai rigoroso e severo.

Invero, il generale sistema di responsabilità e sanzioni introdotto dal legislatore nell'ambito della privacy è sembrato eccessivamente severo ed al contempo non particolarmente efficace, poiché tende ad ampliare a dismisura il campo di applicazione delle sanzioni senza assicurare che le stesse colpiscano i soggetti effettivamente responsabili di un trattamento illecito concretamente nocivo per l'interessato. Ad ogni modo, l'inadeguata o mancata adozione delle misure minime ed idonee, che sia causa di un danno, comporta l'applicazione dell'art. 18 L. n. 675/96, secondo cui "chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile".

L'ambito di applicazione della norma risulta decisamente vasto, considerando:

- l'ampiezza della nozione di trattamento ex art. 2 lett. b) L. n. 675/96 ("qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati");

- la genericità del soggetto imputabile ("chiunque");
- la gravosità del riferimento all'art. 2050 cod. civ., concernente la responsabilità civile oggettiva per attività pericolosa e l'inversione dell'onere della prova a carico del presunto danneggiante;
- la risarcibilità anche del danno non patrimoniale, ai sensi dell'art. 29 c. IX L. n. 675/96.

La dottrina osserva che il riferimento all'art. 2050 cod. civ. non implica che il presunto trattamento illecito sia di per sé un'attività pericolosa, ma piuttosto tende a stabilire che la prova liberatoria non può risolversi nella dimostrazione della mancata violazione delle norme, nell'impiego della diligenza media del buon gestore di banche dati e neppure nella mera adozione delle misure minime. Piuttosto, tale prova dovrebbe accertare l'inclinazione del titolare a porre in essere provvedimenti efficaci alla luce dello stato attuale della tecnologia e congrui in relazione ad una valutazione razionale dell'organizzazione.

Riguardo ai soggetti imputabili, sicuramente in caso di negligenza possono essere coinvolti in modo solidale il titolare, il responsabile e l'incaricato, però la corresponsabilità potrebbe non ricorrere in altre fattispecie concrete, nelle quali emerga una condotta dolosa al livello operativo dell'incaricato, un inadeguato sistema di designazioni da parte del titolare o una palese inattività del responsabile.

Diversamente da quanto previsto per le misure idonee, la violazione dell'obbligo di adozione delle misure minime di sicurezza comporta, ai sensi dell'art. 36 L. n. 675/96, anche la responsabilità penale, con reclusione fino ad un anno o, in caso di danno non commesso per colpa, da due mesi a due anni. La norma, criticabile per l'equiparazione dell'ipotesi colposa a quella dolosa (non dannosa), sembra avere una applicazione più limitata sul piano soggettivo della precedente, atteso che il destinatario della sanzione dovrebbe essere prevalentemente ravvisato nel titolare e/o nel responsabile, a seconda del caso di specie.

6. L'ADOZIONE DELLE MISURE DI SICUREZZA NEGLI STUDI PROFESSIONALI

L'adozione delle misure di sicurezza implica evidentemente un intervento fattivo sull'ambiente di lavoro e le procedure interne. Tale operazione deve essere affrontata con la massima razionalità e coerenza, al fine di raggiungere un adeguato connubio tra efficacia (=piena rispondenza alla legge) ed efficienza (=contenimento dei costi di adeguamento e del rischio di eccessivo irrigidimento delle procedure).

Poiché le misure sia minime che idonee tendono alla riduzione massima dei rischi associati al trattamento dei dati, il titolare deve in ogni caso dimostrare competenza e diligenza nel predisporle. Poiché il processo di adeguamento non si risolve nel compimento di azioni definitive ed immodificabili, è opportuno strutturare gli interventi secondo un piano logico e controllabile a posteriori, al fine di poter gestire in modo agevole e consapevole i successivi aggiornamenti e miglioramenti.

La prima fase della pianificazione degli interventi concerne l'individuazione della strategia di sicurezza. Non essendo disponibili tempi per adottare un approccio progressivo al problema, la strategia deve necessariamente essere orientata al perseguimento, in tempi immediati, della corretta applicazione della legge, ricorrendo a soluzioni a costo relativamente contenuto ma suscettibili di miglioramento nel medio termine.

Alla luce di tale missione, la seconda fase riguarda l'effettuazione di un'analisi sistematica e documentabile dei rischi, con cui definire la probabilità di eventi avversi nel trattamento dei dati personali. In questo momento analitico bisogna procedere all'identificazione degli elementi da proteggere, del rischio intrinseco (deteriorabilità fisica, facilità di smarrimento, guasto tecnico, facilità di accesso e consultazione) e del grado di esposizione effettivo alle avversità.

Nel caso di trattamenti non automatizzati, gli elementi meritevoli di tutela sono gli atti informativi su personale e clienti, le carte di lavoro dalle quali sia identificabile il cliente, i documenti finali aventi destinazione esterna, la corrispondenza e i contatti con la clientela, i curriculum vitae di tirocinanti e le schede informative dei dipendenti. Nei trattamenti automatizzati, invece, meritano attenzione i database, i file di riconciliazione e verifica di saldi e movimenti contabili e le e-mail, residenti tanto sull'hard disk degli elaboratori quanto su supporti rimovibili (floppy disk, cd rom).

Il rischio intrinseco dei primi trattamenti è alto, perché spesso si tratta di materiale originale o manoscritto e facilmente deteriorabile o smarribile; però, l'esposizione reale può non essere altrettanto elevata, quando si stabiliscano semplici regole di collocazione e prelievo dei documenti e si valuti come modesta l'incidenza di fattori esterni di rischio (criminalità nel circondario dello studio, tasso di frequentazione e criminalità nello stabile, incidenza statistica degli atti di vandalismo o di intrusione fisica ai danni di studi professionali, presenza o meno di personale delle pulizie in orari più rischiosi).

Più delicata è la situazione dei documenti informatici, atteso che, nella classificazione dei sistemi informativi adottata dal DPR. n. 318/99, anche un singolo PC provvisto di modem e collegamento ad Internet per mezzo dell'ordinaria linea telefonica rientra nella nozione di "rete disponibile al pubblico" ed è, pertanto, meritevole del massimo grado di sicurezza.

In tal caso, i fattori di rischio sono il danno fisico da vicino (furto o guasto dell'elaboratore con perdita dei dati residenti), il danno logico da vicino (errore umano nella manipolazione dei dati) e il danno logico da remoto (intrusione di terzi via Internet, sottrazione di dati da parte di terzi via Internet, virus). Evidentemente, l'esposizione è tanto più alta quanto minori sono le protezioni tecnologiche sugli elaboratori e minore è l'alfabetizzazione informatica di professionisti e personale.

Sul punto, va notato che conservare i dati su supporti rimovibili riduce, da un lato, il rischio di perdita irreversibile di dati, ma dall'altro aumenta il complesso degli elementi da proteggere, sicché non conviene abusare nella duplicazione dei file e – procedendo ad implementare congrue misure di sicurezza – è consigliabile assumere, come ulteriore precauzione, l'abitudine di eliminare a fine giornata qualsiasi dato riservato dai supporti portatili. Ovviamente, ciò non vale per i supporti contenenti i file eseguibili dei programmi e delle applicazioni specifiche eventualmente usati nello studio, poiché tali elementi non hanno alcuna rilevanza ai fini della normativa in esame.

La terza e la quarta fase del piano di sicurezza sono rappresentate dalle politiche della sicurezza e dal programma operativo, che consentono, rispettivamente, di definire il grado di rischio residuale ritenuto accettabile e di assumere le azioni idonee a contenere i rischi entro il livello stimato. È a questo punto che devono essere:

- assunte e/o verificate le decisioni in fatto di attribuzione di ruoli e qualifiche;
- graduate le attività più critiche e problematiche ai fini della privacy;
- individuate le aree logistiche e le procedure dello studio più critiche e problematiche ai fini della privacy;
- implementate misure di sicurezza di tipo sia formale-documentale che tecnico-organizzativo.

Il tema delle cd. "designazioni" non si risolve nel solo ambito della sicurezza informativa e non può essere affrontato integralmente in questa sede. Tuttavia, limitatamente agli aspetti in esame, si rammenta che:

- con l'Autorizzazione Generale al trattamento dei dati sensibili n. 4 sulle libere professioni, il Garante ammette che in uno studio professionale vi sia una situazione di titolarità del trattamento in capo al professionista ovvero in capo allo studio (se di tipo associato), oppure di contitolarità tra più professionisti legati da un rapporto associativo o di altra natura;
- il responsabile (o i responsabili) va scelto per le sue capacità analitiche, organizzative e di controllo, sovrintende il trattamento ma è privo di veri poteri decisionali e, quindi, non può ricevere alcuna delega di potere o di responsabilità dal titolare;

- in caso di assistenza tecnica oppure di esternalizzazione parziale o totale di trattamenti, è possibile ed anzi opportuno nominare responsabile il referente esterno che appresti tali servizi;
- ciascun incaricato deve poter accedere solo ai dati che sono strettamente necessari allo svolgimento dei compiti affidatigli, sicché è impossibile procedere a definire le singole autorizzazioni senza definire chiaramente le mansioni dei diversi elementi del personale;
- l'amministratore di sistema - che può coincidere o meno con il custode delle parole chiave e deve gestire il sistema informativo, compreso il profilo della sicurezza – dovrebbe identificarsi con il responsabile solo negli studi più piccoli, al fine di evitare un sovraccarico di competenze in capo ad un unico soggetto;
- tutte le designazioni devono essere redatte per iscritto in forma libera e conservate con diligenza, ad esempio raccogliendole in apposito manuale con fogli – anche estraibili – protocollati e numerati.

La mappatura dei processi richiede una riflessione sul carattere e la composizione dell'attività complessivamente condotta dallo studio, in modo da individuare quei servizi meritevoli di particolare attenzione ed ai quali destinare la quota più significativa dell'investimento di adeguamento. Dunque, la ricognizione delle attività maggiormente critiche discende dal giudizio mediato di tre diverse dimensioni, quali l'incidenza dei dati personali per tipo di "prodotto", l'intensità dei dati personali presenti in quello e l'incidenza di quello sul volume d'affari dello studio.

In astratto, è ragionevole ritenere che le registrazioni contabili di tipo analitico, l'assistenza tributaria e del lavoro, la gestione delle fatturazioni e le procedure concorsuali siano le attività nelle quali la gestione delle informazioni presenta diversi profili critici, donde l'opportunità di verificare la relativa sicurezza delle procedure abitualmente seguite nelle varie fasi dell'espletamento di quel tipo di incarico professionale. In tale momento si inserisce la valutazione delle criticità logistiche poco o per nulla compatibili con le norme sulla sicurezza informativa: si tratta, in sostanza, di definire una serie di accorgimenti in grado di controllare meglio il flusso documentale interno allo studio.

Anzitutto, non sembra conforme al DPR n. 318/99 la consolidata abitudine di conservare su scrivanie e tavoli di lavoro faldoni e cartelle relative ai diversi clienti o a singole pratiche riconducibili agli stessi. La documentazione cartacea va piuttosto archiviata in "accessi selezionati o controllati" quali armadi e bacheche oppure, con minore diligenza, mensole elevate: non sembra che sia assolutamente imprescindibile dotare tali accessi di serratura o altri dispositivi più costosi, qualora si adottino cautele non meno valide, come la regola di chiudere le finestre e la porta del locale ove i dati risiedono in caso di assenza o allontanamento del soggetto autorizzato a trattarli.

Comunque, non pare consigliabile che un incaricato disponga di una serie di archivi per cliente o tipo di servizio, poiché ciò contrasterebbe con la sua funzione meramente esecutiva e la sua posizione subalterna. Piuttosto, una parte degli archivi potrebbe essere disposta nell'area ove risiede colui che, tra il titolare ed il responsabile, è meno coinvolto nella ricezione di clienti e contatti esterni e può svolgere l'attività di supervisione, autorizzazione e controllo degli accessi del personale ai dati.
Piuttosto che concepire singole azioni disgiunte l'una dalle altre, potrebbe essere opportuno valutare una revisione del layout complessivo dello studio ed optare per una redisposizione di aree e spazi: il vantaggio di tale approccio risiede nella sua attitudine ad introdurre in modo più sistematico le misure di sicurezza, richiedendo un semplice spostamento delle strutture attuali interne allo studio e solo in via marginale l'acquisto di accessori e nuove dotazioni. Infatti, spesso la configurazione degli studi professionali è il prodotto di scelte assunte a seguito di mutamenti nelle condizioni di espletamento del lavoro - come l'ingresso di ulteriore personale amministrativo, l'introduzione di un maggiore numero di tirocinanti, l'adozione della forma associativa o l'instaurazione di collaborazioni part-time con altri professionisti – in modo contingente e con i tempi spesso serrati imposti dalla stagionalità dell'attività professionale.
La razionalizzazione delle aree di lavoro dovrebbe tendere verso una distinzione logistica dei trattamenti automatizzati "in rete" da quelli "non in rete" e non automatizzati: ciò sarebbe particolarmente rispondente all'art. 5 c. I DPR. n. 318/99, che impone – con riguardo al trattamento dei dati sensibili - l'autorizzazione (=designazione scritta) anche degli "strumenti (=elaboratori) che possono essere utilizzati per l'interconnessione mediante reti disponibili al pubblico". L'individuazione di una struttura dedicata alle elaborazioni elettroniche, quasi una sorta di piccolo c.e.d. - consente evidenti vantaggi, quali la separazione del sistema informativo dal flusso di clienti o di soggetti esterni che accede allo studio, il controllo sulla pertinenza ai compiti assegnati delle attività condotte ai terminali dagli incaricati e la delimitazione fisica dell'intervento in studio del personale di manutenzione ed assistenza tecnica.
I profili operativi finora esaminati assicurano un'adeguata protezione fisica degli archivi cartacei ed elettronici e concorrono a rendere le modalità di lavoro interne più strutturate e controllabili dal punto di vista procedurale e qualitativo. Un discorso a parte merita la sicurezza logica, da vicino e da remoto, che è necessario conseguire relativamente al sistema informativo e che comporta inevitabilmente l'acquisizione di adeguate dotazioni software e/o hardware.
Poiché i dottori commercialisti sono obbligati ad effettuare l'inoltro delle dichiarazioni fiscali per via telematica ed i servizi on line sono sempre più importanti per le libere professioni, è lecito supporre

che nella prevalenza degli studi vi sia almeno un PC collegato ad Internet, per cui si applicano tutte le disposizioni del DPR n. 318/99 in fatto di protezione di terminali contenenti informazioni riservate. Il primo aspetto da regolare è la sicurezza logica da vicino, relativamente alla quale la predisposizione di una parola chiave all'avvio del PC (o password di BIOS) è sufficiente solo in presenza di condizioni praticamente non verosimili, quali l'assenza di dati sensibili e l'unicità del soggetto utilizzatore della macchina.

Mancando tali requisiti, occorre inserire codici utente e password personali per ciascun utilizzatore del PC. Tale operazione richiede che l'elaboratore disponga di uno specifico software oppure di un sistema operativo dotato della stessa funzionalità: poiché il sistema operativo attualmente più diffuso (Microsoft Windows 95/98) consente l'immissione di profili personali banali e facilmente aggirabili, allo scopo di contenere i costi sembra preferibile installare ed acquistare la licenza di un sistema operativo che preveda la gestione in multiutenza – come Microsoft Windows 2000 o NT oppure i sistemi Linux e Unix.

La letteratura tecnica raccomanda alcune semplici regole di definizione delle password, le quali devono essere a base ampia (8 caratteri), alfanumeriche, prive di caratteri ripetuti, non riferite ad elementi del soggetto cui si riferiscono (data di nascita, gusti particolarmente evidenti, nomi di parenti o cari, soprannomi) e tali da formare non vocaboli esistenti, bensì acronimi o sigle. In merito ai codici ed alle password, particolare rilievo assume la figura del custode, appositamente designato per registrare tali informazioni, accertarsi che più soggetti non usino né contemporaneamente né in tempi diversi le medesime chiavi di accesso e disattivare i diritti di accesso rimasti inutilizzati dal beneficiario per un periodo superiore a sei mesi.

Il ruolo del custode delle password diventa ulteriormente significativo quando sia anche adottata la precauzione, consigliabile, del cambiamento periodico di codici e password di tutti gli utenti. Altri accorgimenti a costo nullo o minimo che gli utenti potrebbero adottare sono:

- l'attivazione della funzione di screen saver con password (da rendere nota a tutti gli utenti autorizzati ad accedere ad un medesimo terminale, se di uso promiscuo);
- l'installazione di piccoli software di compressione dei file (come Winzip o Winrar) – prelevabili da Internet con licenza gratuita temporanea o acquistabili a prezzi assolutamente modici - che consentono di salvare il lavoro compiuto in archivi cancellabili ma inaccessibili, perché muniti di password.

Il secondo aspetto da considerare nella protezione dei dati personali residenti nel sistema informativo è la sicurezza logica da remoto, rispetto alla quale il DPR richiede l'impiego di programmi idonei a

contrastare intrusioni telematiche. Il riferimento, in prima analisi, è ai programmi virus, in grado di cancellare il contenuto della memoria permanente dell'elaboratore o, addirittura, di rendere inutilizzabile l'hardware; tuttavia, le intrusioni possono anche essere compiute dai cd. "pirati informatici" che impiegano apposti software per accedere, per motivi specifici o casualmente, a sistemi informativi altrui, consultando o distruggendo i dati in quelli contenuti.

Per contrastare il pericolo dei virus informatici è sufficiente acquistare (con modica spesa) ed installare un programma antivirus con relativa licenza, avendo cura di scaricare periodicamente on line gli aggiornamenti gratuiti delle definizioni dei nuovi virus riscontrati sul Web dalla software house.

Contro il rischio di accessi abusivi da parte di navigatori di Internet, sono invece disponibili programmi (software) e dispositivi (hardware) di protezione dei terminali, detti firewall, che operano come un filtro tra il PC locale e la rete mondiale, selezionando le richieste di contatto in base a criteri predefiniti.

Per gli studi non particolarmente grandi e con sistemi informativi non molto complessi, può essere sufficiente l'acquisto e l'installazione di un firewall di tipo software, che non è impossibile reperire on line con licenza temporanea gratuita. In ogni caso, potrebbe essere necessaria l'assistenza tecnica per impostarne la regolazione in modo efficace.

Il DPR n. 318/99 richiede la verifica almeno semestrale dello stato di efficacia ed aggiornamento di tutte le dotazioni anti-intrusione da remoto.

La quinta ed ultima fase del ciclo della sicurezza concerne adempimenti obbligatori - la revisione delle misure (auditing) e le iniziative di formazione interna – e l'adozione facoltativa di misure a carattere divulgativo, come l'affissione nello studio di una breve nota esplicativa per clienti e personale recante:

- l'indicazione, ove necessario nominativa, dei soggetti presenti nello studio e del ruolo assunto rispetto alla normativa sulla privacy;
- informazioni minimali sulle misure tecnico-organizzative implementate ai fini della sicurezza dei dati trattati;
- i diritti esercitabili dall'interessato;
- regole semplici e dirette – che non ricalchino semplicemente le norme di legge, inevitabilmente generali - per il personale.

Quest'ultimo tipo di provvedimento è, peraltro, idoneo a configurare un'iniziativa di formazione e sensibilizzazione permanenti del personale e dei collaboratori dello studio in materia di riservatezza.

Un profilo delicato relativo all'implementazione delle misure di sicurezza è la predisposizione di evidenze in grado di documentare, ai fini probatori, il corretto adempimento degli obblighi previsti

dalla L. n. 675/96 e dal DPR. n. 318/99. Infatti, la libertà di forma insita nelle disposizioni inerenti le misure di sicurezza – che costituiscono pur sempre atti interni all'organizzazione del titolare del trattamento – e l'assenza di espliciti vincoli non impongono al titolare di adottare particolari cautele formali nell'attuazione del piano di sicurezza. Tuttavia, in considerazione dei poteri ispettivi del Garante e della particolare gravosità dell'inversione dell'onere della prova prevista in sede di responsabilità civile, è opportuno che il titolare provveda il più possibile a documentare la propria attività.

7. PRECISAZIONI CONCLUSIVE SUL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

L'art. 6 DPR n. 318/99 prevede, nel caso di organizzazioni dotate di una rete disponibile al pubblico e contenente trattamenti di dati sensibili e giudiziari, l'obbligo della stesura e della revisione almeno annuale del documento programmatico sulla sicurezza (DPS). La norma non descrive nel dettaglio il contenuto e la valenza del documento, ma lascia intendere - insieme ad alcune precisazioni del Garante - che si tratti di un atto non sintetico e di carattere non meramente tecnico-informatico.
Infatti, il DPS è un vero e proprio documento pianificatorio e complessivo, che deve definire:

- "i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;
- i criteri e le procedure per assicurare l'integrità dei dati;
- i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica;
- l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni".

L'elemento più significativo del DPR n. 318/99 è costituito dall'ultima parte dell'art. 6 c. I, laddove si stabilisce che gli aspetti sopraelencati devono essere individuati "sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi". Questo appunto caratterizza in modo palese la vocazione sistematica del DPS ed il suo stretto rapporto con il complessivo piano di sicurezza dei dati personali, fornendo oltretutto una conferma all'approccio analitico e tecnico-operativo adottato ed esposto nel presente documento.

Quindi, l'implementazione delle misure di sicurezza nello studio del dottore commercialista deve trovare adeguata visibilità ed esposizione anche nel DPS, il quale si pone in posizione dialettica rispetto alle misure concretamente realizzate, in quanto: da un lato, i provvedimenti posti in essere trovano la loro origine e previsione nel DPS; dall'altro, quest'ultimo deve ricevere tutti i mutamenti e gli aggiornamenti correlati alle esigenze di modificazione e revisione delle misure nel tempo adottate.

Stampato presso la sede della Fondazione – maggio 2001