

### Audizione

del Presidente di ConfProfessioni Gaetano Stella presso gli Uffici di Presidenza congiunti delle Commissioni speciali per l'esame degli atti urgenti presentati dal Governo di Camera e Senato, sull'Atto del Governo n. 22 (Adeguamento normativa nazionale circa la protezione delle persone fisiche con riguardo al trattamento dei dati personali).

Giovedì 31 maggio 2018

Illustri Presidenti, Onorevoli Deputati e Senatori,

Giunge al Vostro esame lo schema di decreto legislativo<sup>1</sup> recante le norme di adeguamento dell'ordinamento italiano al nuovo Regolamento europeo sulla protezione dei dati personali. Il decreto delegato – che si perfeziona **a ridosso dell'entrata in vigore del Regolamento europeo**, avvenuta pochi giorni fa, ed entra in vigore retroattivamente assieme al Regolamento – **interviene in modo massiccio sul Codice della Privacy**<sup>2</sup>, ora novellando le sue disposizioni in attuazione del Regolamento europeo, ora abrogandole in quanto incompatibili o ripetitive di norme direttamente applicabili dello stesso.

In forza della sua diretta applicabilità negli ordinamenti degli Stati membri, **il Regolamento europeo viene dunque a rappresentare la nuova fonte di riferimento della materia**, integrata dal Codice della *Privacy*, come novellato, per i profili sui quali il Regolamento espressamente prevede, o comunque implica, una normativa statale di attuazione. Questo riassetto delle fonti – conseguenza della scelta di mutare lo strumento normativo in ambito europeo, passando dalla previgente Direttiva al Regolamento –

---

<sup>1</sup> Il decreto è adottato in base alla delega di cui all'art. 13 della legge 25 ottobre 2017, n. 163, «Delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE».

<sup>2</sup> D. Lgs. 196/2003.

determina una potenziale sovrapposizione di norme che il decreto al Vostro esame è chiamato ad ordinare.

1. A fronte della vastissima mole di temi e problemi che una normativa tanto complessa e articolata propone, il contributo che ConfProfessioni può portare al Vostro dibattito concerne **l'impatto delle nuove misure per la protezione dei dati personali sugli studi professionali**. Ed infatti, gli studi professionali sono – al pari delle amministrazioni pubbliche e delle aziende – tra i destinatari della nuova normativa, anche qualora rivestano dimensioni molto circoscritte e individuali. **Il considerando 13 del Regolamento, infatti, include le micro-imprese tra i destinatari del provvedimento**, facendo espresso riferimento alla raccomandazione 2003/361/CE della Commissione, che a sua volta ha operato un'equiparazione tra liberi professionisti e piccole e medie imprese. Ne deriva che anche i professionisti, in qualità di titolari o responsabili del trattamento, devono adottare misure organizzative e tecniche idonee a garantire un livello di sicurezza adeguato al rischio sia informatico che legale, legato al trattamento del dato.

Al contempo, tuttavia, **il considerando 13 del Regolamento** invita le istituzioni europee e degli Stati membri «a **considerare le esigenze specifiche delle micro, piccole e medie imprese** nell'applicare il presente regolamento».

Lo schema di decreto legislativo al vostro esame ha preferito rimettere al Garante l'apprezzamento di queste esigenze, affidandogli **il potere di «promuovere, nel rispetto delle disposizioni del Regolamento e del presente decreto, modalità particolari di adempimento degli obblighi del titolare del trattamento, funzionali ad esigenze di semplificazione delle micro, piccole e medie imprese»** (cfr. art. 22, comma 10, dello schema di decreto).

Benché collocata ai margini del decreto, nelle sue disposizioni finali, la norma ora citata riveste **un'importanza cruciale per gli operatori economici di medie e piccole dimensioni, e certamente per gli studi professionali**. Sulla base dei dati raccolti e diffusi dal nostro “Osservatorio delle Libere Professioni”, in Italia i professionisti sono più di 2 milioni; nella maggior parte dei casi, operano in organizzazioni monoprofessionali o comunque di ridotte dimensioni: il numero medio di dipendenti è di 2,7 per studio professionale. Già da questi dati emerge con evidenza che ci troviamo di fronte a una realtà economica la cui *compliance* con le finalità del nuovo Regolamento potrà avvenire solo se instradata attraverso processi di semplificazione.

Riteniamo pertanto essenziale che il Parere parlamentare che Vi accingete a redigere possa segnalare l'utilità di ulteriori specificazioni di questa norma, e comunque rappresentare l'urgenza che **il Garante si disponga ad un confronto con le parti sociali interessate** per configurare una prima normativa applicabile alle piccole e medie imprese. Una delega tanto ampia e indeterminata al Garante per una quota tanto rilevante degli operatori economici italiani può avere senso solo se diretta a recepire i contenuti di una normativa condivisa, in sintonia con i principi del Regolamento europeo. Una regolamentazione condivisa, dunque, che noi auspichiamo altresì: (i) **dettagliata** settore per settore, con particolare attenzione alle peculiarità degli studi professionali rispetto alle imprese che operano in altri settori, e in grado di specificare gli adempimenti professione per professione, giacché diversa è la tipologia dei

dati e il livello di trattamento cui sono sottoposti i commercialisti o i notai rispetto ai medici o ai veterinari; nonché (ii) **tempestiva**, per impedire il protrarsi dell'applicazione della normativa generale anche ai soggetti meritevoli di condizioni differenziate. Infatti, il protrarsi dell'applicazione della disciplina generale anche a realtà incongruenti potrebbe determinare effetti negativi sulle attività economiche, che si traducono in maggiori oneri, adempimenti, costi, responsabilità e certamente in distonia con i principi del Regolamento europeo.

Due sono gli obiettivi strategici a cui, a nostro avviso, la disciplina indirizzata agli studi professionali dovrebbe ispirarsi: la promozione dell'**autoregolamentazione** attraverso lo strumento del codice di condotta e la **semplificazione** degli adempimenti.

2. Al fine di adeguare la normativa in commento alla realtà specifica delle professioni regolamentate in forma ordinistica, riteniamo anzitutto essenziale ricorrere alla redazione di appositi **codici di condotta per il trattamento e la protezione dei dati personali**, quali strumenti che favoriscano processi di *accountability* dei professionisti e di adeguamento spontaneo ai principi e alle regole in materia di protezione dei dati. Il codice di condotta è individuato dal considerando 98 e dall'**art. 40 del Regolamento** quale strumento idoneo a facilitare l'applicazione del Regolamento «tenendo conto delle caratteristiche specifiche dei trattamenti effettuati in alcuni settori e delle esigenze specifiche delle microimprese», nonché a calibrare i metodi di protezione nei singoli settori. I codici possono dunque garantire un corretto bilanciamento tra tutela dei diritti fondamentali, da un lato, ed esigenze specifiche dell'organizzazione economica, dall'altro, evitando altresì che regole e modelli organizzativi calati dall'alto – e pensati per soggetti economici più complessi ed articolati – possano essere imposti a realtà economiche più circoscritte e molto diverse tra loro.

L'art. 40 del Regolamento europeo prevede che i codici di condotta prendano forma all'interno di un dialogo tra organi pubblici e associazioni rappresentative degli operatori del settore, secondo un processo di confronto pubblico-privato che è a nostro avviso particolarmente apprezzabile. È pertanto necessario che le norme di condotta in tema di trattamento e protezione dei dati personali vengano elaborate attraverso una **concertazione che coinvolga il Garante e le libere associazioni dei professionisti del settore**; e che essa prenda corpo in un **codice *ad hoc***.

3. Con riferimento ai contenuti specifici del Regolamento europeo, la normativa che auspichiamo possa prendere forma in attuazione del comma 10 dell'art. 22 del decreto dovrà mirare all'obiettivo di **semplificare gli adempimenti**, in coerenza con le dimensioni organizzative degli studi professionali.

In via preliminare rileviamo che i presidi introdotti dal Regolamento appaiono in larga parte condivisibili, specie perché volti a controllare processi sempre più frequenti nel mondo economico, di raccolta e trasmissione dei dati personali, e profilazione ed uso degli stessi a scopo commerciale. Nel porsi questo obiettivo, il Regolamento peraltro introduce un sistema di protezione improntato alla adeguatezza dei metodi rispetto alle dimensioni e alla natura dei soggetti economici, esprimendo in più occasioni l'intenzione di non approntare un modello unitario e vincolante, ma di responsabilizzare i soggetti economici circa il livello di protezione da garantire. Questo approccio – che per le micro-imprese ha preso corpo nelle

disposizioni menzionate, da cui si è ricavata l'esigenza di una disciplina derogatoria – è stata definita «*accountability*». Per quanto concerne gli studi professionali, ferma la libertà degli studi di adottare specifici piani ed organigrammi di tutela, articolati in modo originale e calati sulle esigenze e sulle caratteristiche del singolo studio, riteniamo essenziale la predisposizione di **un modello organizzativo generale**, a cui i professionisti siano chiamati ad adeguarsi, con la forza di assorbire la responsabilità del singolo professionista anche in casi di violazioni verificatesi nonostante il rispetto delle prescrizioni, secondo il modello della responsabilità d'impresa di cui al D. Lgs. 231/01. Ribadiamo che il modello organizzativo per la tutela della *privacy* negli studi professionali – necessariamente agile e semplificato – **debba maturare all'esito di un processo di autoregolamentazione ai sensi dell'art. 40 del Regolamento europeo**, dunque condotto dalle associazioni in dialettica con il Garante, per ciascuna professione. Lasciare in capo al singolo professionista l'onere di approntare un modello organizzativo di prevenzione del rischio connesso al trattamento dei dati può comportare un abbassamento del livello di protezione effettivo, e l'esposizione dei professionisti a carichi di lavoro, ad esternalizzazioni, e dunque a costi del tutto incongruenti con la loro realtà organizzativa.

Alcuni dei presidi approntati dal Regolamento possono certamente essere accolti anche nel modello organizzativo per gli studi professionali: è il caso, per esempio, della **valutazione preliminare del rischio**, che il professionista svolge già, implicitamente, al momento dell'assunzione dell'incarico professionale; lo stesso può dirsi per l'adeguamento delle prassi relative all'ottenimento del **consenso al trattamento dei dati** e alle relative **informative sui diritti dell'utente**, che devono essere rese al cliente. Anche in questo caso, siamo in presenza di processi tipici della dialettica tra professionista e utente, che in diverse situazioni sono già formalizzate. A tal fine, è di ausilio la circostanza che l'incarico professionale è ora conferito in forma scritta, attraverso la sottoscrizione del preventivo, che in base alle recenti normative deve rivestire la forma scritta<sup>3</sup>. Spetta pertanto all'autoregolamentazione che auspichiamo possa essere avviata dal Garante approntare modelli procedurali che affianchino alla predisposizione del preventivo economico da sottoporre al cliente, anche un'adeguata informativa sulla *privacy* e, sull'altro lato della scrivania, la responsabilizzazione del professionista nella valutazione preliminare del rischio.

Diversa la valutazione con riferimento ai presidi approntati dal Regolamento, evidentemente calati sulla realtà delle grandi aziende, che implicano oneri di carattere organizzativo, di risorse e di personale in capo all'operatore economico.

È lo stesso Regolamento ad escludere, per le organizzazioni con meno di 250 dipendenti l'obbligo di tenuta del **Registro dei trattamenti**. È di tutta evidenza che gli studi professionali – anche quelli più complessi e strutturati in forma societaria – non cadono nel perimetro di applicazione di questa misura di tutela.

Più complessa l'analisi per la normativa che istituisce il **Data Protection Officer (DPO)**, la cui presenza viene ritenuta obbligatoria in quelle strutture la cui attività implichi un trattamento di dati sensibili **su «larga scala»** (art. 37 Regolamento).

---

<sup>3</sup> Cfr. l. 124/17.

La nozione è decisamente ambigua, e ha dato luogo sin da subito a commenti divergenti. Nelle sue FAQ, tuttavia, il Garante della *Privacy* ha escluso che i caratteri del trattamento su larga scala possano rinvenirsi nella realtà dei professionisti operanti in forma individuale. Ed in effetti, la dimensione «su larga scala» emerge, tuttalpiù, all'interno di strutture complesse, quali cliniche e ospedali o redazioni giornalistiche, in cui i professionisti operano in base a contratti di lavoro o di collaborazione, ma senza la diretta responsabilità del trattamento dei dati. Vi è da aggiungere che gli studi professionali, anche quando giungano, tramite organizzazioni più complesse, ad incamerare masse di dati sensibili ingenti, non operano mai nell'obiettivo di aggregare i dati, individuare *trend*, profilare risposte sulla base di dati: i professionisti operano sempre al servizio dell'utente, i cui **dati sensibili sono destinati a rimanere "isolati"** rispetto alle altre attività del professionista. Sono considerazioni che dovrebbero spingere a risolvere negativamente anche il quesito circa l'estensione dell'obbligo di istituzione del DPO anche nelle strutture professioni complesse, quali le Società tra professionisti o gli studi associati di maggiori dimensioni.

Non c'è dubbio, comunque, che una soluzione univoca di interpretazione della norma potrà essere offerta in sede di adozione della normativa di cui al comma 10 dell'art. 22 del decreto legislativo, in modo tale da escludere la sussistenza di questo obbligo in capo ai soggetti libero-professionali, i cui **obblighi di tutela rispetto a dati sensibili possono comunque essere adeguatamente assolti facendo leva su modelli – adottati in sede di autoregolamentazione e in dialogo col Garante – meno onerosi sotto il profilo dello sforzo organizzativo** e più coerenti con le tradizioni di una categoria che da sempre gestisce dati sensibili degli utenti, senza che ciò abbia determinato violazioni gravi o sistematiche.

Anche le norme in materia di **"Data breach"** – modellate sulla realtà dei grandi operatori che gestiscono banche dati di dimensioni e diffusione globale – appaiono del tutto incongruenti rispetto agli studi professionali. Ipotizzare che in caso di "furto" di un dato, o di "accesso illecito" ad una banca dati di uno studio professionale si debba avviare un meccanismo di allarme che coinvolge il Garante appare sinceramente sproporzionato.

È peraltro vero che gli studi talora conservano dati sensibili su persone fisiche e giuridiche di particolare notorietà e rilievo – dati di potenziale interesse per rivali, concorrenti, *media*, ecc. –, da preservare dunque con massima cura. I codici di autoregolamentazione che auspichiamo possano essere adottati potranno senz'altro dettagliare i doveri dei professionisti in tali casi e le relative sanzioni.

\* \* \*

Illustri Presidenti, Onorevoli Deputati e Senatori,

il Regolamento europeo sulla protezione dei dati personali e il decreto legislativo oggi al Vostro esame per il prescritto parere parlamentare configurano un impianto normativo estremamente complesso, che tuttavia è nel suo insieme apprezzabile. Esso affronta sfide imponenti della società della comunicazione e della informatizzazione, prospettando l'Europa come ambiente all'avanguardia nella tutela dei diritti fondamentali della persona.

Si tratta, al contempo, di preservare le peculiari modalità organizzative di alcune strutture economiche, che possono adeguarsi agli obiettivi della normativa in modo diverso, più congruente con le loro dimensioni organizzative. È questo, peraltro, lo spirito del Regolamento europeo, come evidenziato nel considerando 13. È certamente così per le professioni regolamentate in forma ordinistica, che presentano caratteristiche del tutto peculiari rispetto al tema che qui ci occupa.

La normativa al Vostro esame si fa carico di queste esigenze con la clausola del comma 10 dell'art. 22, che rimette al Garante la determinazione di una normativa derogatoria per le piccole e medie imprese e quindi per i liberi professionisti. È assai utile che il Parere al Vostro esame indirizzi il Governo prima, e il Garante stesso poi, nell'attuazione di questa norma, apparentemente tanto generica e libera nelle forme e nei contenuti. Indirizzi che a nostro avviso debbono concretizzarsi (i) nella semplificazione degli adempimenti, con particolare riguardo al DPO e ai casi di *Data Breach*, e (ii) nella promozione dell'autoregolamentazione attraverso il codice di condotta, che rispecchia al contempo le finalità del nuovo Regolamento europeo (art. 40).

È in questo spirito, di contemperamento degli interessi, che anche i liberi professionisti possono contribuire allo sviluppo della normativa e delle prassi in un settore tanto delicato per il nostro futuro, quale l'integrità dei dati personali.