POSITION PAPER

IL NUOVO REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

A cura dell'Ufficio legislativo e relazioni istituzionali CNA

Premessa

Il 4 maggio 2016 è stato pubblicato nella Gazzetta Ufficiale dell'Unione europea il nuovo **Regolamento (UE) 2016/679** del Parlamento europeo e del Consiglio (noto come GDPR - *General Data Protection Regulation*) relativo alla **protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati**.

Tale provvedimento abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), da cui è disceso il decreto legislativo 30 giugno 2003, n. 196 (c.d. Codice in materia di protezione dei dati personali).

Si tratta di una piccola rivoluzione nel mondo della privacy. Il suo percorso, però, è risultato in continua salita. Nato con l'intento di regolarizzare soprattutto le attività di *marketing* e profilazione svolte dai grandi gruppi societari, rischia di penalizzare le piccole imprese, che in un Paese come l'Italia costituiscono l'ossatura e il traino del sistema economico.

LA DISCIPLINA IN TEMA DI PRIVACY PRIMA E DOPO IL REGOLAMENTO	
L'AMBITO DI APPLICAZIONE DELLA DISCIPLINA SULLA PRIVACY	
PRIMA	**DOPO**
La normativa europea è stata applicata con riferimento al Paese membro in cui aveva sede il titolare del trattamento dei dati.	Il Regolamento presenta un ambito applicativo più esteso, concernendo ogni tipo di trattamento posto in essere da un titolare o responsabile presente nel territorio dell'UE. Parimenti, in ipotesi specifiche, si applica al trattamento di dati personali di interessati che si trovano nell'UE che sia effettuato da un titolare o da un responsabile del trattamento non stabilito nell'Unione (art. 3).

L'APPROCCIO AL TRATTAMENTO DEI DATI PERSONALI	
PRIMA	**DOPO**
La direttiva del 1995 e il Codice italiano sono stati elaborati su un preponderante approccio documentale, prevedendo in quest'ottica la notifica preventiva dei trattamenti all'autorità di controllo e la verifica preliminare (c.d. *prior checking*).	Perno centrale del Regolamento diventa il principio della responsabilizzazione (*accountability*) finalizzato alla verifica dei rischi inerenti al trattamento per i diritti e le libertà degli interessati. Tutti i soggetti responsabili del trattamento sono chiamati a decidere autonomamente modalità, garanzie, limiti e, più in generale, le misure propedeutiche al trattamento, vale a dire la raccolta, la conservazione, l'uso e la protezione dei dati (Capo IV del Regolamento). Il processo di *accountability* si realizza attraverso alcuni criteri indicati dal Regolamento quali la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita (art. 25) e soprattutto la valutazione di impatto sulla protezione dei dati (art. 35). All'esito di questa valutazione il titolare decide se iniziare o meno il trattamento ovvero consultare il Garante, il quale, intervenendo solo *ex post*, indica misure ulteriori o correttive (art. 58).
LE CARATTERISTICHE DELL'INFORMATIVA	
PRIMA	**DOPO**
L'informativa è apparsa nella pratica ricca di rimandi normativi e tendenzialmente complessa. L'interessato era informato oralmente o per iscritto circa le finalità e le modalità del trattamento, la natura obbligatoria o facoltativa del conferimento dei dati, le conseguenze di un eventuale rifiuto a rispondere, i soggetti o le categorie di soggetti ai quali i dati personali potevano essere comunicati, i diritti, gli estremi identificativi del titolare e del responsabile.	L'informativa deve risultare concisa, trasparente, intelligibile, accessibile, nonché articolata mediante un linguaggio semplice e chiaro. Va fornita all'interessato per iscritto o con altri mezzi come quelli elettronici. L'informativa può essere resa anche in combinazione ad icone standardizzate per offrire un quadro d'insieme del trattamento previsto. Ad ogni modo, i contenuti dell'informativa sono elencati in modo tassativo e appaiono più ampi che in precedenza (Artt. 12, 13 e 14).

IL CONSENSO	
PRIMA	**DOPO**
Si è ammesso il trattamento dei dati personali solo con il consenso espresso dell'interessato. Il consenso, alla stregua di quanto accadrà dal 25 maggio prossimo, doveva essere libero, specifico e informato.	Il consenso deve corrispondere ad una manifestazione di volontà libera, specifica, informata e inequivocabile. Il consenso può essere espresso attraverso una dichiarazione ovvero tramite una azione positiva, mentre la richiesta di consenso deve essere distinguibile da altre richieste rivolte all'interessato. Il titolare del trattamento deve essere in grado di dimostrare che l'interessato abbia prestato il proprio consenso, anche quando non è prestato per iscritto (artt. 4 e 7).
IL TITOLARE DEL TRATTAMENTO, IL RESPONSABILE DEL TRATTAMENTO E IL RESPONSABILE DELLA PROTEZIONE DEI DATI	
PRIMA	**DOPO**
Non è stata prevista la figura del responsabile della protezione dei dati. Per quanto riguarda, invece, le caratteristiche soggettive e le rispettive responsabilità di titolare e responsabile restano sostanzialmente le medesime.	Rispetto alla precedente normativa il Regolamento: introduce la possibilità di ricorrere alla contitolarità del trattamento nel rispetto di un accordo interno che disciplini il rispettivo ambito di responsabilità (art. 26); fissa più dettagliatamente le caratteristiche del contratto con cui il titolare designa un responsabile del trattamento, consentendo a quest'ultimo il ricorso a sub-responsabili previa autorizzazione del titolare (art. 28); in casi tassativamente previsti, stabilisce la designazione di un responsabile della protezione dei dati (c.d. DPO – *Data Protection Officer*), la cui figura riflette l'approccio responsabilizzante che è proprio del Regolamento (art. 37).

LA VIOLAZIONE DEI DATI PERSONALI	
PRIMA	**DOPO**
Non è stato necessario che il titolare comunicasse eventuali violazioni nel trattamento dei dati all'autorità di controllo. Successivamente il Garante aveva previsto con autonomi provvedimenti l'obbligo di notificazione per società telefoniche ed *internet provider*, enti pubblici, dossier sanitario, elettronico e biometria.	In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo. Tuttavia, la violazione deve comportare un rischio per i diritti e le libertà delle persone fisiche, la cui valutazione è rimessa ancora una volta al titolare (art. 33). Soltanto quando la violazione in questione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare ne dà comunicazione all'interessato (art. 34).
IL RICONOSCIMENTO DEI DIRITTI	
PRIMA	**DOPO**
I diritti che hanno tutelato l'interessato in merito alla gestione dei propri dati hanno denotato una estensione piuttosto circoscritta.	I diritti tutelati dal Regolamento vengono rafforzati: il diritto di accesso riconosce all'interessato il diritto di ricevere in ogni caso una copia dei dati personali oggetto del trattamento (art. 15); il diritto alla cancellazione dei propri dati personali (c.d. diritto all'oblio) prevede che i titolari che abbiano reso pubblici dati personali debbano informare gli altri titolari che trattano i medesimi dati e su cui pende la richiesta di cancellazione (art. 17); il diritto di ottenere dal titolare la limitazione del trattamento offre maggiori garanzie rispetto al blocco del trattamento (art. 18); il diritto alla portabilità dei dati rappresenta infine un nuovo diritto previsto dal Regolamento (art. 20).
IL QUADRO SANZIONATORIO	
PRIMA	**DOPO**
La normativa precedente ha introdotto per la prima volta diverse fattispecie sanzionatorie che in larga parte vengono confermate dal nuovo quadro sanzionatorio.	Secondo quanto previsto dal Regolamento, mentre la materia penale è rimessa alla competenza di ciascun Stato membro dell'Unione, le sanzioni amministrative pecuniarie vanno irrogate dalle relative

	autorità di controllo in base ai criteri di effettività, proporzionalità e dissuasività. Le misure sanzionatorie debbono essere applicate in funzione del singolo caso, tenendo conto, per la definizione del loro ammontare, di alcuni parametri: la natura, la gravità e la durata della violazione, le finalità del trattamento, il numero di interessati lesi e il livello del danno, nonché altri elementi tra cui il carattere doloso o colposo della violazione, il riscontro di eventuali precedenti violazioni e il grado di cooperazione sviluppato con l'autorità di controllo per porre rimedio ai possibili effetti negativi della violazione (art. 83). I limiti massimi stabiliti dalla nuova disciplina per gli importi delle sanzioni risultano comunque elevati (fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale annuale).

CRITICITA' E PROPOSTE	
La valutazione d'impatto sulla protezione dei dati	Il Regolamento indica tra i nuovi obblighi spettanti ai titolari nonché agli eventuali responsabili del trattamento la «valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali» (art. 35, par. 1). Tale onere ricade nella sfera di responsabilità del titolare/responsabile nella misura in cui il trattamento, allorché preveda in particolare l'uso di nuove tecnologie, comporti un **rischio elevato** per i diritti e le libertà delle persone fisiche. Soltanto in questo caso il titolare è chiamato ad effettuare una valutazione preventiva d'impatto che descriva il trattamento dei dati, pesi la necessità ed il metodo, contribuisca alla gestione dei rischi determinando le misure necessarie ad affrontarli. Ad ogni modo, il Garante ha la possibilità di **individuare** nei fatti quali **soggetti siano da esonerare dall'obbligo di realizzare la predetta valutazione**, giacché non effettuerebbero trattamenti rischiosi. Infatti, la normativa stabilisce come l'autorità di controllo possa redigere e rendere pubblico «un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati» (art. 35, par. 5). Stando così le cose, ci si chiede come mai non sia stata ancora sfruttata dal Garante questa straordinaria opportunità di chiarezza che fornirebbe un quadro di riferimento certo ed eviterebbe alle imprese di procedere alla verifica d'impatto anche quando non dovuta. Invece, sul sito del Garante della privacy si può attingere soltanto da qualche settimana ad un mero collegamento che rinvia al portale dell'Autorità francese per la protezione dei dati (CNIL), la quale ha messo a disposizione un software di ausilio per la valutazione d'impatto sulla protezione dei dati, senza che costituisca un modello a cui fare riferimento in ogni situazione.
Il registro delle attività di trattamento	Il Regolamento introduce un'ulteriore adempimento. Prevede infatti che i titolari e i responsabili del trattamento annotino su un apposito registro le operazioni relative al trattamento dei dati personali (art. 30, parr. 1 e 2), ma **esclude che le imprese con meno di 250 dipendenti siano vincolate alla tenuta di detto registro** (art. 30, par. 5). Tuttavia, quest'ultima deroga non si applica, con conseguente riespansione degli effetti della regola generale, allorché il trattamento: a) presenti un **rischio** per i diritti

	e le libertà dell'interessato; b) **non sia occasionale**; c) o **includa categorie particolari di dati** di cui all'art. 9 (origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) ovvero **dati personali relativi a condanne penali e reati** di cui all'art. 10. Occorre che il Garante precisi la portata dell'art. 30, par. 5, del Regolamento. **La disposizione necessita infatti di una interpretazione che tenga conto delle dimensioni dell'impresa e dell'entità delle attività poste in essere**. All'inverso, lasciando che si insinui una interpretazione eccessivamente lasca ed estensiva, si corre il rischio che il gravame colpisca molte di quelle micro o piccole imprese che trattano in maniera estemporanea informazioni specifiche per soddisfare le richieste della clientela, senza che tali informazioni siano concretamente utilizzabili per altri fini (si pensi ad una parrucchiera che acquisisca l'informazione di una allergia di una cliente rispetto alla somministrazione di un determinato cosmetico).
Il responsabile della protezione dei dati	L'art. 37, par. 1, del Regolamento obbliga il titolare o il responsabile del trattamento alla designazione del responsabile della protezione dei dati (DPO - *Data Protection Officer*) per assolvere funzioni di supporto e controllo, consultive, formative e informative circa l'applicazione della nuova normativa. La designazione avviene in presenza delle seguenti ipotesi: a) il trattamento è effettuato da un'autorità pubblica; b) le attività principali del titolare del trattamento o del responsabile consistono in trattamenti che per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; c) le attività principali del titolare del trattamento o del responsabile consistono nel trattamento, su larga scala, di categorie particolari di dati personali (art. 9) o di dati relativi a condanne penali e a reati (art. 10). Al di fuori di questi casi, il titolare o il responsabile del trattamento **possono comunque designare** un responsabile della protezione dei dati (art. 37, par. 4). Il Regolamento prescrive dunque la designazione del responsabile della protezione solo per ipotesi tassativamente previste, permettendo in ogni caso la discrezionale designazione di questa figura in tutte le ipotesi non obbligatorie. Ciononostante si sta

	facendo strada una interpretazione in base a cui sarebbe sempre conveniente individuare tale responsabile, indipendentemente dal coefficiente di pericolosità del trattamento e della relativa protezione. D'altra parte, lo stesso Garante, nelle FAQ sul responsabile della protezione dei dati in ambito privato, dopo aver dispensato dalla designazione sia le imprese individuali o familiari che le piccole e medie imprese, raccomanda alla luce del principio di *accountability* la designazione del responsabile. Sicché, si chiede al Garante che ci si attenga ad una corretta interpretazione dell'art. 37 per cui **la designazione**, **ove non necessaria**, **deve restare facoltativa**, in modo da liberare le imprese da oneri non richiesti e rifuggire da una preoccupante situazione che rischia di precipitare in uno stato di confusione e allarmismo.
I codici di condotta	Il Regolamento prescrive inoltre che Stati membri, autorità di controllo, comitato europeo per la protezione dei dati e Commissione europea debbano incoraggiare l'elaborazione di **codici di condotta**. Tali soggetti sono chiamati a contribuire alla corretta applicazione del Regolamento, «in funzione delle specificità dei vari settori di trattamento e delle **esigenze specifiche delle micro**, **piccole e medie imprese**» (art. 40, par. 1). Allo scopo di precisare l'applicazione del presente regolamento, le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento «possono elaborare i codici di condotta, modificarli o prorogarli» e sottoporre il relativo progetto all'autorità di controllo competente per l'eventuale parere di conformità e il conseguente *placet* sull'intero progetto di codice, modifica o proroga (art. 40, parr. 2 e 5). Ove approvati dal Garante e validati dalla Commissione europea, i titolari o i responsabili del trattamento possono aderire ai predetti codici (art. 40, parr. 3 e 9). A dispetto però di quanto disciplinato dalla normativa europea, l'autorità italiana per la protezione dei dati personali non ha dato impulso ad un reale **percorso di coinvolgimento che contempli la partecipazione di associazioni e rappresentanti di micro**, **piccole e medie imprese**. Pertanto, si chiede al Garante di attivare al più presto un tavolo tecnico con le predette realtà per elaborare delle proposte che avviino alla stagione dei codici di condotta, fortemente improntati alla semplificazione amministrativa.
La proroga dell'entrata in	Alla luce dei **ritardi accumulati dal Governo** nella adozione del decreto legislativo teso ad adeguare la normativa nazionale al

vigore delle sanzioni	Regolamento UE 2016/679 del 27 aprile 2016 e delle **incertezze mostrate dal Garante** nella definizione di una puntuale cornice interpretativa di sussidio alle imprese, appare opportuno riflettere su un dato di fondo in vista della sua imminente applicazione (25 maggio p.v.). La normativa in questione si prepara ad entrare in vigore in un clima in cui serpeggia il malumore, il senso di sfiducia e il timore per le nuove sanzioni (art. 83). In questo quadro, le imprese invocano legittimamente flessibilità nei controlli e una più stretta collaborazione con il Garante della privacy. Di conseguenza, sul modello del periodo di grazia già ottenuto in sede europea dalla Francia, si chiede la concessione di una **fase transitoria di sei mesi nel corso della quale non potranno essere irrogate sanzioni alle imprese** che, a seguito di ispezioni, siano rimaste indietro rispetto ai nuovi adempimenti. In altri termini, appare opportuno concedere un lasso minimo di tempo per consentire ai soggetti interessati di completare i propri piani di adeguamento alla nuova normativa ed evitare quindi di incorrere in sanzioni considerevolmente onerose. In tal senso, nell'ambito dell'esame dello schema di decreto legislativo che adegua la normativa nazionale alle disposizioni del regolamento in esame, risulta doveroso inserire la proroga sulle sanzioni.