

GDPR

La regolazione amministrativa del trattamento dei dati personali

di Giuliano Fonderico

L'applicazione del Reg. n. 2016/679/UE (GDPR) spinge in avanti l'armonizzazione della disciplina dei trattamenti dei dati personali, offre nuovi strumenti di controllo per gli interessati e accentua i connotati "amministrativi" delle regolazioni pubbliche coinvolte. Il Regolamento conforma per vari aspetti le organizzazioni, i processi e i meccanismi decisionali dei soggetti dei trattamenti, allestendo un modello di regolazione con tratti precauzionali e *risk-based*. Nonostante il ricorso allo strumento regolamentare, al legislatore nazionale spetta un compito gravoso di adeguamento e integrazione della normazione interna, che potrebbe avere influssi significativi anche su numerosi segmenti di azione amministrativa.

La tutela "amministrativa" dei dati personali: dalla Dir. n. 95/46/CE al Reg. n. 2016/679/UE

La Dir. 95/46/CE ha rappresentato per lungo tempo la disciplina di riferimento in materia di dati personali. Essa ha segnato alcune scelte di fondo in relazione ai fini, all'oggetto, e ai modelli della tutela dei dati personali.

La direttiva ha anzitutto riunito una duplice finalità. Quella più immediata, legata alla sua base giuridica (l'art. 100 A del Trattato CE allora vigente) consisteva nell'armonizzazione dei regimi nazionali sul trattamento dei dati. L'individuazione di un livello di tutela equivalente era necessaria affinché i dislivelli di regolazione su base nazionale non creassero ostacoli alla circolazione dei dati e, per effetto, allo sviluppo del mercato interno. Come è accaduto spesso nel diritto della Comunità e poi dell'Unione, però, il

ravvicinamento non è stato un'operazione neutrale rispetto agli interessi coinvolti ma esso stesso ha elevato tali interessi nella sfera del giuridicamente protetto. Nello scegliere il livello comune di tutela, la direttiva ha ricavato dalle legislazioni nazionali già esistenti, dai "principi del diritto comunitario" e dal diritto alla protezione della vita privata già affermato dall'art. 8 della Convenzione CEDU l'esigenza di attestarsi su una soglia "elevata" (v. il considerando 10). Con l'ulteriore conseguenza che tale soglia è divenuta quella minima da garantire ma anche quella massima oltre la quale i singoli Stati membri non potevano andare (1).

Quanto all'oggetto della tutela, la direttiva ha superato sin dal principio una concezione più risalente basata sulla protezione della sola sfera di riservatezza individuale, della quale è peraltro espressione proprio l'art. 8 della Convenzione CEDU (2). La direttiva vi aggiungeva una visione più ampia diretta a dotare gli

(1) Con riferimento alla Dir. 95/46/CE, la Corte di giustizia ha affermato che "l'armonizzazione delle suddette legislazioni nazionali non si limita quindi ad un'armonizzazione minima, ma sfocia in un'armonizzazione che, in linea di principio, è completa. È in quest'ottica che la direttiva 95/46 intende garantire la libera circolazione dei dati personali, pur assicurando un alto livello di tutela dei diritti e degli interessi delle persone cui si riferiscono tali dati" (Corte di giustizia 24 novembre 2011, *Asnef*, in cause riunite C-468/10 e C-469/10, punto 29; conforme, v. già, Corte di giustizia 6 novembre 2003, *Lindqvist*, in causa C-101/01, punto 96). La Corte, riferendosi all'art. 7 della direttiva con un ragionamento estendibile a tutti i principi contenuti nella direttiva, ha concluso: "Ne consegue che gli Stati membri non possono né aggiungere nuovi principi relativi alla legittimazione del trattamento dei dati personali all'art. 7 della direttiva 95/46, né prevedere requisiti supplementari che vengano a

modificare la portata di uno dei sei principi previsti da detto articolo" (punto 32 della sentenza *Asnef*).

(2) La disposizione della Convenzione si limita a prevedere, al comma 1, che "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza". Al comma 2 la norma stabilisce limiti all'ingerenza dei poteri pubblici in tale sfera di riservatezza, secondo una logica simile a quella delle garanzie costituzionali in materia. Per una "costituzionalizzazione" del diritto alla protezione dei dati personali, per come inteso dalla direttiva 95/46, occorre attendere la Carta dei diritti fondamentali dell'Unione europea, all'art. 8, e il Trattato sul funzionamento dell'Unione europea, all'art. 16. Sul carattere innovativo, e non meramente ricognitivo, della disposizione della Carta, cfr. G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Vienna, Springer, 2014.

“interessati” - *i.e.*, le persone alle quali i dati personali si riferiscono - di un certo grado di controllo sui loro dati personali e sui trattamenti che ne vengono fatti. Questo tipo di tutela, almeno nella sua formulazione di base, non risentiva del grado di confidenzialità dei dati né del loro contenuto, se non per l'eventuale attrazione in regimi di maggior rigore, come ad esempio è accaduto per le “categorie particolari” di dati (art. 8 della Dir. 95/46/CE), che nella legislazione nazionale sarebbero poi stati qualificati come “sensibili” (art. 22 della L. n. 675/1996). L'attribuzione di una sfera di controllo non è stata intesa in senso proprietario, come pure era stato suggerito sul piano dell'analisi economica per promuovere il raggiungimento di equilibri “efficienti” nel trattamento dei dati (3). Da un lato, il controllo sui dati da parte dell'interessato non è pieno perché, per varie ragioni, i dati possono essere trattati anche senza il suo consenso. Dall'altro lato, i trattamenti non sono leciti solo perché compiuti con il consenso dell'interessato, occorre comunque il rispetto dei principi sul trattamento e il consenso è sempre revocabile. Gli interessati non possono dunque disporre dei loro dati personali con piena autonomia negoziale.

Le scelte sulle situazioni tutelate hanno avuto sin dal principio un influsso sul modello di disciplina. La direttiva conteneva prescrizioni coerenti con la protezione della sfera di riservatezza individuale, concentrate intorno alla definizione di diritti, obblighi e divieti nel rapporto tra gli interessati e i soggetti dei trattamenti. L'estensione del controllo a ogni possibile impiego dei dati e la natura non disponibile della situazione tutelata portavano però a forme di intervento più intense e preventive, fondate su prescrizioni organizzative (es., le misure di sicurezza, la disciplina dei rapporti con i responsabili; artt. 16 e 17) e adempimenti (es., la notifica e il registro dei trattamenti; artt. 18 e 21). Ciò ha avuto un riflesso amministrativo nella previsione di “autorità di controllo” nazionali le quali, oltre a fornire tutela in via amministrativa per le situazioni individuali, sono divenute assegnatarie di poteri inibitori e conformativi che hanno prefigurato una più generale funzione di vigilanza amministrativa sulle attività di trattamento dei dati (v. l'art. 28).

Questa componente della disciplina è restata tuttavia sotto traccia, anche per la marcata caratterizzazione delle situazioni tutelate in termini di diritti fondamentali. Le norme di recepimento nel nostro ordinamento hanno seguito la medesima impostazione, tradottasi ad esempio nella previsione di poteri coercitivi dell'autorità di controllo limitati - almeno all'apparenza - ai rapporti tra specifici soggetti dei trattamenti e gli interessati (4) e nell'estensione della giurisdizione ordinaria a ogni genere di provvedimento delle autorità di controllo (5), non solo agli atti di cura dei “diritti” di singoli interessati.

Il profilo amministrativo dell'attività di controllo si è però ugualmente sviluppato. A livello europeo, con l'adozione di direttive settoriali che hanno intensificato la conformazione organizzativa e funzionale già ricavabile dalla Dir. 95/46/CE. È il caso della Dir. 2002/58/CE sulla protezione dei dati personali nelle comunicazioni elettroniche e in particolare delle sue previsioni in tema di misure di sicurezza e di violazione dei dati personali (v. l'art. 4, per come modificato dalla Dir. 2009/136/CE). A livello nazionale, facendo leva su aspetti pressoché incidentali della disciplina. Da un lato, il potere di “segnalazione” sin dal principio attribuito al Garante per la protezione dei dati personali (6) ha visto una sorta di evoluzione spontanea verso un potere di adottare prescrizioni generali (7). In virtù di esso, il Garante ha adottato nel tempo numerosi “provvedimenti generali” per concretizzare i principi della disciplina in misure organizzative, adempimenti, limiti di contenuto, tempo, estensione ecc. ai trattamenti realizzabili. Dall'altro lato, la disciplina nazionale ha introdotto forme di “auto regolazione”, i cc.dd. codici deontologici, sottoposte in realtà a un intenso controllo amministrativo dall'avvio sino alla conclusione del procedimento e con efficacia prescrittiva generale, estesa *ex lege* a chiunque effettui i trattamenti regolati (art. 12, D.Lgs. n. 196/2003) (8). In questo modo, il corpo di principi e regole previsto dalle norme - sino al codice della riservatezza del 2003 - si è arricchito di numerose regolazioni amministrative, orizzontali e per settori, con ricadute significative sull'organizzazione e sull'attività dei soggetti dei trattamenti.

Il Reg. n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR) ha sviluppato in più direzioni le scelte

(3) V. ad esempio R.S. Murphy, *Property rights in personal information: an economic defense of privacy*, in *Geo. L. J.*, 84, 1996, 2381.

(4) V. l'art. 31, L. n. 675/1996.

(5) V. l'art. 29, comma 8, L. n. 675/1996.

(6) Art. 31, comma 1, lett. c, L. n. 675/1996.

(7) Art. 154, comma 1, lett. c), D.Lgs. n. 196/2003, che il richiamo all'art. 143 sembrerebbe circoscrivere alle decisioni sui reclami da parte di singoli interessati ma che il Garante ha interpretato come espressione di un potere di regolazione generale.

(8) Cfr., per un tentativo d'inquadramento nei fenomeni di c.d. *soft law*, E. Mostacci, *La soft law nel sistema delle fonti: uno studio comparato*, Padova, 2008, 145 ss.

iniziali della direttiva. Esso ha anzitutto spinto in avanti l'armonizzazione, per l'appunto con la scelta di passare alla fonte regolamentare per sua natura non bisognosa di norme di recepimento. Peraltro, su vari temi, specie quelli legati all'azione dei pubblici poteri, il Regolamento ammette o richiede discipline integrative da parte degli Stati membri (v. ad esempio l'art. 6, par. 2) e dunque prefigura un quadro che potrebbe conservare un buon grado di eterogeneità. Il Regolamento ha senz'altro accentuato la focalizzazione della tutela sul controllo dell'uso dei dati personali. Ne sono un esempio alcuni "nuovi" diritti degli interessati, come ad esempio quello c.d. all'oblio o quello alla portabilità dei dati personali. Il Regolamento, infine, ha ricostruito in un quadro organico la componente "amministrativa" della precedente disciplina, attingendo soluzioni anche da norme che nel frattempo erano state adottate per singoli settori, come la Dir. 2002/58/CE sopra citata. Ciò è avvenuto sviluppando una serie di istituti che erano già presenti nella Dir. 95/46/CE e accompagnandoli con figure organizzative e modelli procedurali di nuova concezione.

L'aspetto unificante degli istituti è che essi conformano l'organizzazione e l'attività dei soggetti del trattamento in quanto tali, anticipando il momento della tutela a prescindere dagli esiti specifici che possono essere raggiunti nei confronti di singoli interessati. Le misure sono volte ad accrescere la c.d. *accountability* dei soggetti dei trattamenti (art. 24), formula che sta a indicare per l'appunto un più generale spostamento dell'attenzione sulla *capacità* dei soggetti del trattamento di rispettare le norme del Regolamento.

Le conformazioni organizzative: l'RPD, le altre figure organizzative e la sicurezza

Una prima serie di conformazioni riguarda l'organizzazione. L'innovazione più significativa del Regolamento

è la previsione del responsabile per la protezione dei dati ("RPD"; artt. 37 ss.). Il responsabile è un ufficio con funzioni consultive e di controllo oltre che di contatto per le autorità di controllo e per gli interessati. Figure simili erano previste dalla legislazione di singoli ordinamenti nazionali (9) e si erano diffuse anche in modo spontaneo, quali centri di imputazione delle funzioni in materia di riservatezza.

Il Regolamento interviene anzitutto sull'istituzione dell'ufficio che è in taluni casi obbligatoria (10), essendone comunque suggerita la nomina per ogni organizzazione che svolga trattamenti dei dati su scala significativa (11). Il Regolamento disciplina i criteri di selezione dell'RPD, ancorati alle qualità professionali e alle competenze specialistiche del responsabile (12), disegnando poi gli aspetti essenziali dello statuto dell'RPD, incentrati sull'indipendenza e autonomia dell'ufficio e sulla disponibilità di risorse sufficienti a svolgere i suoi compiti.

Sul piano dei rapporti organizzativi, il titolare dell'ufficio di RPD non deve essere sottoposto ai poteri di direttiva o d'istruzione da parte di altri organi del soggetto dei trattamenti in merito all'esercizio delle funzioni proprie di RPD, direttive o istruzioni del genere non devono essere impartite neppure concretamente. L'indipendenza implica anche che l'RPD non possa essere rimosso o penalizzato in ragione delle sue funzioni. Il suo rapporto, in ogni caso, deve avere un minimo di stabilità nel tempo. Sul piano delle dotazioni dell'ufficio di RPD, esse - in termini umani e materiali - devono essere sufficienti a espletare i compiti previsti. L'ufficio deve ricevere la collaborazione degli altri uffici del soggetto dei trattamenti ed essere adeguatamente e periodicamente formato.

Il Regolamento crea così un ufficio che, nell'espletamento delle sue funzioni, è sottratto all'indirizzo degli organi di governo del titolare dei trattamenti e che

(9) V. il *Bundesdatenschutzgesetz* tedesco, Sez. 4f, sul *beauftragter für den datenschutz*.

(10) Talune ipotesi sono ancorate principalmente a dati formali e non dovrebbero porre problemi applicativi particolari. Le autorità e gli organismi pubblici, ad eccezione delle autorità giurisdizionali, sono senz'altro tenute alla nomina di un responsabile. Allo stesso modo, sono tenuti a designare un RPD i titolari del trattamento che come attività principale trattino su larga scala dati "particolari" (art. 9 del regolamento, ad esempio dati relativi alla salute) o attinenti a condanne penali e a reati (art. 10 del regolamento). Potrebbe essere il caso di strutture sanitarie private o di soggetti che svolgono su larga scala attività difensive o investigative in ambito penale. Una terza ipotesi è quella delle entità la cui attività principale consiste "in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala". Potrebbe ricadere nell'ipotesi un operatore di comunicazioni con un'infrastruttura che genera stabilmente una mole significativa di dati pertinenti agli interessati, come ad esempio i dati di traffico.

(11) Nei casi dubbi, quando cioè non sia evidente che un soggetto non sia tenuto alla nomina dell'RPD, le linee guida del Gruppo 29 sul responsabile della protezione dei dati (WP 243 rev. 01) chiedono di esplicitare e documentare l'analisi seguita per giungere alla conclusione di non istituire l'RPD (par. 2.1.). Anche nei casi dubbi sembrerebbe dunque privilegiarsi l'istituzione della figura, salvo un'argomentata scelta in senso contrario.

(12) Visto che i compiti specifici dell'RPD attengono all'applicazione del regolamento e alla disciplina della riservatezza, la qualità professionale principale richiesta all'RPD è quella pertinente a tale disciplina e alla sua applicazione. Si tratta, in altri termini, di una competenza professionale di tipo *orizzontale*, in sé autonoma rispetto al particolare settore di attività del soggetto dei trattamenti. Nondimeno, specie per le attività che abbiano maggiore complessità, anche tecnologica, sono utili altresì conoscenze di tipo *settoriale* sull'attività che svolge il soggetto dei trattamenti e sulle esigenze di sicurezza che la caratterizzano (si v. le citate linee guida sull'RPD, par. 2.4.).

idealmente dovrebbe agire come interprete neutrale delle norme sulla riservatezza, anche in posizione dialettica rispetto agli organi di amministrazione del titolare. Di qui l'esigenza che, ove l'RPD rivesta anche altri ruoli, non vi sia tra tali funzioni un conflitto di interessi di tipo organizzativo, che cioè l'RPD non debba pronunciarsi sugli atti che esso stesso compie in altra veste (art. 38, par. 6) (13). Nella pratica, con l'intensificarsi delle relazioni tra gli RPD e le autorità di controllo e il diffondersi di "comunità epistemiche" degli RPD, la figura potrebbe accentuare ancora di più tali tratti.

Il Regolamento contiene alcune novità anche sul tema della distribuzione dei ruoli nei trattamenti, tra il titolare e il responsabile dei trattamenti, intendendosi per tale il soggetto che tratta i dati "per conto" del titolare (14). In questo caso, più che un ufficio autonomo, si ha un regime applicabile al ricorrere di ogni genere di rapporto che per l'appunto implichi il trattamento dei dati per conto del titolare. Si pensi alle innumerevoli figure di esternalizzazione che caratterizzano le moderne organizzazioni imprenditoriali, strutturate spesso come centri di coordinamento di "fasci di contratti". In simili circostanze, la qualificazione di un fornitore come "responsabile dei trattamenti" sarà essenzialmente ricognitiva di un determinato assetto negoziale.

Il Regolamento, riprendendo quanto previsto dalla direttiva, prevede anzitutto i criteri di selezione del "responsabile", dovendo quest'ultimo avere caratteristiche tecniche e organizzative adeguate a garantire il rispetto della riservatezza dei dati. Il responsabile deve essere legato al titolare da un contratto o altro atto giuridico vincolante, così come era previsto già dalla direttiva (art. 17, par. 3). Il Regolamento prevede però una disciplina molto più dettagliata del contenuto del rapporto (art. 28), codificando una serie di soluzioni che, nel vigore della direttiva, erano state elaborate dalla prassi per regolare il caso delle nomine di sub-responsabili (v. l'art. 28, par. 4). Nel nuovo quadro, il responsabile dei trattamenti deve assistere il titolare in tutti i principali obblighi organizzativi e procedurali e

vi deve essere una perimetrazione molto accurata dei trattamenti che gli sono affidati, delle modalità nelle quali devono essere svolte e dei relativi controlli da parte del titolare. Tali aspetti hanno un rilievo decisivo anzitutto per il titolare. Essi rilevano per valutare la tenuta complessiva del suo modello organizzativo e il grado di responsabilità nel caso di condotte del responsabile non conformi al Regolamento. Dall'altro lato, la delimitazione dell'affidamento incide sulla stessa qualificazione come "responsabile". Quest'ultimo, se opera al di fuori dei trattamenti affidati e per finalità difformi da quelle indicate dal titolare, va considerato a sua volta come un autonomo titolare dei trattamenti (art. 28, par. 10).

Nell'insieme, il Regolamento non preclude di organizzare le attività - economiche o meno che siano - distribuendole tra una rete di soggetti autonomi legati da rapporti contrattuali. Esso però incide sulla scelta delle controparti e integra il contenuto del rapporto, ponendo di fatto alcuni limiti alle forme organizzative più complesse. Nel caso ad esempio dei rapporti a cascata il Regolamento impone che vi sia una continuità negoziale, seppure indiretta, tra il titolare e la catena dei sub responsabili (art. 28, par. 4). Questo collegamento prescinde dalle condizioni legali o negoziali dei fenomeni sub contrattuali e va modellato seguendo il flusso dei dati trattati per conto del titolare.

Un impatto più complessivo sull'organizzazione delle entità che svolgono trattamenti viene dalle prescrizioni in tema di sicurezza (art. 32) e di minimizzazione dei trattamenti (art. 25). Previsioni analoghe erano già contenute nella direttiva (v. l'art. 17 sulle misure di sicurezza) o comunque si potevano desumere da principi da essa affermati, come il principio di necessità (art. 6, par. 1, lett. c) dal quale si ricavava la limitazione dei trattamenti al minimo occorrente per perseguire finalità legittime (v. l'art. 3 del D.Lgs. n. 196/2003). Il Regolamento esplicita le ricadute più puntuali del principio di necessità e le sviluppa in varie direzioni, per garantire la protezione dei dati come criterio interno ai trattamenti (*privacy by*

(13) Le funzioni congiuntamente imputate al titolare dell'ufficio di RPD devono essere tali da non entrare tra loro in collisione anche a prescindere dagli interessi personali dell'RPD. Questo potrebbe accadere, ad esempio, se l'RPD fosse titolare di un ufficio sottoposto al controllo dell'RPD stesso. L'imputazione di più funzioni, in secondo luogo, non deve essere tale da lasciare all'RPD risorse insufficienti per esplicare i suoi compiti.

(14) Il regolamento non contempla espressamente l'ipotesi di un responsabile interno, aspetto che ha sollevato il dubbio se tale soluzione - sin qui diffusa nella prassi - sia ancora ammissibile o se invece si debba ricorrere ad altri schemi come la delega di funzioni proprie del titolare. V., in questo secondo senso, lo schema di

decreto delegato per l'attuazione del regolamento, con l'art. 2-terdecies che verrebbe inserito nel D.Lgs. n. 196/2003. In realtà, così come accadeva nella Dir. 95/46/CE (art. 2, lett. e), il regolamento comprende nella nozione di responsabile anche le persone fisiche, i servizi o altri organismi che trattano i dati per conto del titolare (art. 4, par. 1, n. 8), dal che non vi sarebbero ostacoli di principio per ipotizzare imputazioni della funzione a elementi organizzativi interni, come ad esempio un ufficio dirigenziale. La circostanza che alcuni elementi della disciplina del responsabile sembrerebbero assumere un'alterità più marcata delle persone non è decisiva, potendo dipendere semplicemente dalla scelta di adottare regole comuni ai due casi.

design) e che i trattamenti coinvolgano - “per impostazione predefinita” - solo i dati necessari per la specifica finalità perseguita (*privacy by default*). Ciò implica l’assunzione di presidi tecnici - ad esempio, tecniche di cifratura e pseudonimizzazione - ma anche un più generale ripensamento delle organizzazioni, dell’articolazione delle competenze e della distribuzione delle conoscenze tra i vari uffici.

La proceduralizzazione: la minimizzazione e la valutazione d’impatto, la sicurezza, i diritti degli interessati

L’altro versante sul quale il Regolamento produce i suoi effetti è la proceduralizzazione delle attività del titolare che comportano il trattamento dei dati. Tale proceduralizzazione è in parte una conseguenza indotta da prescrizioni di altra natura. Si è visto, ad esempio, che il Regolamento prevede il principio di “minimizzazione” dei trattamenti anzitutto come regola di organizzazione del titolare (art. 25). Il principio, nondimeno, va coordinato con gli ordinari processi di sviluppo delle attività del titolare, si pensi al disegno di nuovi prodotti e servizi nell’ambito di attività imprenditoriali. È verosimile che la *privacy by design* e *by default* siano integrate stabilmente in tali processi, divenendo una sorta di sub processo nel quale si definiscono le nuove attività anche in relazione ai trattamenti dei dati che implicano. L’aspetto procedurale è enfatizzato dal possibile coinvolgimento di uffici specializzati, come l’RPD, in funzione consultiva.

Lo stesso può dirsi per la “violazione dei dati personali”, vale a dire “la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati” (art. 4, n. 12). Il fenomeno era stato già disciplinato nell’ambito dei servizi di comunicazione elettronica nell’ambito della Dir. 2002/58/Ce, il Regolamento ha esteso la soluzione a tutte le attività di trattamento. In presenza di una violazione, il titolare è tenuto a compiere una serie di attività di verifica delle cause e mitigazione degli effetti nonché, in parallelo, a comunicare l’evento all’autorità di controllo e, secondo le circostanze, anche agli interessati i cui dati siano coinvolti nella violazione (artt. 33-34). Il Regolamento stabilisce una tempistica molto stretta - 72 ore al massimo per la prima comunicazione all’autorità di controllo - la quale include al suo interno anche i tempi che eventualmente possono occorrere per i flussi d’informazione tra il titolare e i suoi responsabili esterni del trattamento, presso i quali potrebbe essere localizzata

la violazione. È dunque pressoché inevitabile che i titolari dei trattamenti diano una veste procedurale alle varie attività, distribuendo tra i propri uffici interni - incluso l’RPD, nel consueto ruolo consultivo - le competenze. La previsione di un modello del genere, del resto, può essere a sua volta considerato un adempimento organizzativo necessario come misura minima di sicurezza.

Una tendenza marcata all’allestimento di procedure dovrebbe essere anche conseguenza della disciplina sui diritti degli interessati, come quelli di accesso, oblio, opposizione, portabilità ecc. (artt. 12 ss.). I soggetti che svolgono i trattamenti sono tenuti a risposte “sollecite” (di regola, nel termine di 30 giorni). In questo lasso di tempo, i diritti degli interessati richiedono la capacità di individuare, estrarre e gestire informazioni puntuali, con i conseguenti aggiornamenti sui sistemi informatizzati e manuali coinvolti nei trattamenti. La capacità di garantire stabilmente tali risultati fa parte delle responsabilità generali del titolare dei trattamenti (art. 24) e, specie nelle organizzazioni di maggiori dimensioni, dovrà confidare su procedure definite in anticipo e dimensionate su previsioni di ricorso agli istituti sottoposte ad affinamenti periodici.

In altri casi, la proceduralizzazione è disposta espressamente dal Regolamento, talvolta sulla falsariga di veri e propri procedimenti amministrativi. Per i trattamenti che prevedendo “l’uso di nuove tecnologie, considerati la natura, l’oggetto, il contesto e le finalità del trattamento, [possono] presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell’impatto dei trattamenti previsti sulla protezione dei dati personali” (art. 35).

I contenuti principali della valutazione sono definiti dal Regolamento, il quale prescrive la consultazione con l’RPD e prevede anche l’apertura del procedimento verso l’esterno, con la consultazione degli interessati (art. 35, par. 9). Il Regolamento dispone una fase di riesame quando vi sia una variazione del rischio (*id.*, par. 11). Sin qui la disciplina si muove nell’ambito dell’autovalutazione. Ove gli esiti di questo primo esame indichino la presenza di rischi elevati e la necessità di misure di attenuazione, il Regolamento prescrive la consultazione preventiva con l’autorità di controllo (art. 36). Si apre così una fase di valutazione amministrativa che si conclude con un “parere” che può essere accompagnato dai provvedimenti inibitori e conformativi di cui all’art. 58 del Regolamento.

Nelle misure di sicurezza che i titolari devono definire rientra “una procedura per testare, verificare e valutare

regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento" (art. 32, par. 1, lett. d). Il titolare dei trattamenti dovrà dunque allestire un processo di revisione periodica con sperimentazioni, controlli e valutazioni che concretamente dovrebbero avvenire secondo classificazioni tipizzate dei livelli di rischio e dei rimedi corrispondenti.

I principi sulle decisioni

Nel modello definito dal Regolamento, l'adeguatezza dell'organizzazione e dei processi costituisce una condizione minima necessaria ma non sufficiente per la correttezza dei trattamenti. Il Regolamento contiene difatti anche principi e regole sulle decisioni in tema di trattamento.

In primo luogo, ogni trattamento deve fondarsi su almeno una delle "basi giuridiche" legittime considerate dal Regolamento. Per esempio, il trattamento è legittimo se è necessario per formare o eseguire un contratto con l'interessato o per adempiere un obbligo di legge, o ancora se è fondato sul consenso dell'interessato (art. 6). Tali basi giuridiche hanno natura formale e operano incondizionatamente, nel senso che, se ricorrono, si può procedere ai trattamenti senza ulteriori valutazioni. Nel nuovo quadro, tuttavia, esse potrebbero avere un ambito applicativo limitato. Le basi giuridiche "contrattuali" e "legali" possono essere azionate solo se i trattamenti sono strettamente necessari alla formazione e all'esecuzione del rapporto o al rispetto dell'obbligo di legge (15). Il consenso, inoltre, può costituire una valida base giuridica solo quando la manifestazione di volontà dell'interessata sia libera da ogni condizionamento. La soglia di "libertà" che sembra prevalere è in effetti alquanto elevata. Si ritiene ad esempio che il consenso non sia di regola validamente prestato nell'ambito dei rapporti di lavoro ma anche in tutti i casi in cui esso non sia sufficientemente distinto per singole tipologie di trattamento (c.d. "granularità") o sia stato richiesto come condizione per ricevere una prestazione di altra natura.

Nel nuovo quadro potrebbe così avere un ruolo più ampio la base giuridica del "legittimo interesse" del titolare. Essa era prevista anche dalla direttiva ma, almeno nel nostro ordinamento, il suo ambito era stato fortemente limitato dalla scelta del legislatore nazionale - peraltro di dubbia compatibilità con la

direttiva - di condizionarne l'applicazione a decisioni preventive puntuali del Garante (art. 24, comma 1, lett. g, D.Lgs. n. 196/2003).

Nel Regolamento la valutazione sull'esistenza di un legittimo interesse è svolta autonomamente dal titolare del trattamento e non è relegata a un ruolo residuale e di chiusura (16). Possono essere considerati legittimi interessi di natura commerciale, come ad esempio quello di un'impresa a informare i propri clienti delle promozioni o dei nuovi prodotti e servizi disponibili (v. il considerando n. 47 del Regolamento). Vi è poi la vasta schiera degli interessi alla difesa della propria sfera giuridica, che possono rilevare sia in via preventiva - si pensi ai modelli organizzativi aziendali per la prevenzione degli illeciti o comunque per garantire una gestione efficiente dell'azienda - sia in via successiva, al momento in cui insorgono controversie.

A differenza dalle altre, la base giuridica del legittimo interesse ha però la peculiarità di richiedere un bilanciamento con gli interessi, i diritti e le libertà fondamentali degli interessati, che non devono essere "prevalenti" rispetto all'interesse del titolare. In concreto, vi potrebbero essere casi in cui il trattamento, seppur fondato su un "legittimo interesse" del titolare, sia comunque lesivo di diritti e libertà fondamentali e dunque non possa essere attuato affatto. Il più delle volte, il bilanciamento degli interessi potrebbe richiedere al titolare di accompagnare i trattamenti con limiti e cautele specifiche, che assicurino la "prevalenza" dei diritti degli interessati. Per un trattamento per finalità commerciali, ad esempio, potrebbe occorrere una limitazione dei canali o delle frequenze di contatto o ancora la previsione di un meccanismo semplificato per opporsi ai trattamenti. Il titolare dovrà così incorporare nella decisione una fase di ponderazione degli interessi della quale occorrerà dare una documentazione e che dovrebbe riflettersi nelle misure associate al trattamento.

In altri casi, il Regolamento incide sui soggetti delle decisioni, limitando la facoltà del titolare di ricorrere a meccanismi automatizzati per decisioni che producono effetti giuridici che riguardano l'interessato o che incidono in modo analogo significativamente sulla sua persona (art. 22, par. 1; v. in precedenza l'art. 15 della direttiva 95/46/CE). Il fenomeno al quale si riferisce la norma è molto ampio e spesso non è percepibile dai

(15) V. le linee guida del Gruppo 29 su *Automated individual decision-making and Profiling for the purposes of Regulation 2016/67* (WP251 rev.01), 12 ss.

(16) V. Gruppo 29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/*

EC (WP 217), 9 ss. Nel senso che, alla luce della giurisprudenza della Corte di giustizia, si debba dare un'interpretazione restrittiva della clausola, cfr. F. Ferretti, *Data protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights?*, in *CML Rev.*, vol. 51, 2014, 843-868.

destinatari. Si pensi ai meccanismi di *credit scoring* nei servizi bancari e finanziari, ai sistemi medici avanzati di diagnosi e prevenzione, a certe valutazioni che possono incidere sulle carriere lavorative. In casi del genere, un certo grado di automatizzazione è inevitabile e consente di accelerare e rendere più efficienti i processi decisionali. I dati sui quali si basano le decisioni, tuttavia, potrebbero essere imprecisi e condurre a scelte errate, cristallizzare condizioni e comportamenti passati, essere fonte di discriminazioni. Il Regolamento si concentra sulle decisioni prese senza un intervento umano effettivo, con algoritmi applicati in modo automatico da sistemi informatici, e che producono “effetti giuridici” immediati o che comunque incidono in modo “significativo” sulle persone. Un esempio del primo caso potrebbe essere il diniego di riconoscimento di un determinato status, come la cittadinanza, la qualità di rifugiato ecc. Un esempio del secondo potrebbe essere il rifiuto di un finanziamento o l'esclusione da una selezione per un impiego.

Non è chiaro se il Regolamento ponga un vero e proprio divieto o attribuisca agli interessati solo la facoltà di opporsi. L'interpretazione sin qui data in ambito UE è nel senso del divieto, anche in assenza di opposizione dell'interessato (17). In ogni caso, il Regolamento lascia spazio per deroghe, ad esempio se il trattamento automatizzato è necessario per eseguire un contratto o se c'è il consenso dell'interessato. L'interessato deve essere informato preventivamente del meccanismo e della sua logica. Esso può chiedere che gli elementi della decisione siano rettificati. Deve potere esprimere la sua opinione e contestare la decisione e ha il diritto di ottenere un “intervento umano” effettivo nel processo decisionale.

Conclusioni e prospettive per il diritto interno

Il GDPR delinea un complesso meccanismo di regolazione delle attività dei soggetti che svolgono trattamenti dei dati personali. Lo fa con prescrizioni immediate e richiedendo l'adozione di modelli organizzativi e procedurali per prevenire trattamenti dei dati personali non conformi alla disciplina, con una logica posta a cavallo tra quella precauzionale e i modelli di

regolazione c.d. *risk-based*. L'apparato sanzionatorio viene riorientato di conseguenza. Il Regolamento, al contrario della direttiva, contiene un proprio sistema di sanzioni pecuniarie che sono applicabili sia a illeciti puntuali sia a disfunzioni organizzative considerate nel loro insieme, come ad esempio, un modello aziendale non rispettoso dei principi generali sul trattamento o difetti di gestione dei rapporti con i responsabili del trattamento. In coerenza con tale impostazione, le sanzioni sono calcolate sul fatturato complessivo dell'impresa e, a certe condizioni, su quello del gruppo di appartenenza, secondo la stessa logica del diritto *anti-trust* UE (18).

La regolazione opera definendo i tratti principali dei modelli, lascia poi a ciascun soggetto di allestire quello più adeguato alla sua organizzazione e alle sue attività. Il Regolamento, inoltre, prefigura lo sviluppo di regolazioni di secondo grado su base volontaria, attraverso meccanismi di certificazione e codici di condotta ad adesione spontanea che consentono ai soggetti dei trattamenti di attestare e verificare periodicamente la conformità delle proprie organizzazioni alle norme. Alle autorità di controllo, anche attraverso lo specifico ufficio di coordinamento del Comitato europeo per la protezione dei dati (art. 68 del Regolamento), spettano poteri di orientamento generale e di decisione puntuale sia sui modelli applicati direttamente dai soggetti dei trattamenti sia sulla formazione e applicazione dei sistemi di certificazione e dei codici di condotta (19). Solo una parte di tali poteri riguarderà la rispondenza di atti e comportamenti a diritti puntualmente definiti degli interessati, per lo più le autorità valuteranno equilibri fra interessi e questioni tecniche e organizzative complesse.

Le caratteristiche di tali meccanismi di regolazione hanno dunque sicuri motivi d'interesse per gli studi di diritto amministrativo, che sino a questo momento hanno per lo più trascurato la disciplina della riservatezza. A ciò deve aggiungersi un aspetto, per così dire, quantitativo, legato alla portata particolarmente ampia del Regolamento. Pressoché tutte le attività pubbliche e private di una qualche rilevanza implicano il trattamento dei dati personali e il Regolamento ha scelto una soluzione tendenzialmente “omnibus” (20).

(17) Cfr. le linee guida del Gruppo 29 in tema di *Automated individual decision-making and Profiling for the purposes of Regulation 2016/67*, 19 ss.

(18) I massimali variano dal 2% al 4% del fatturato mondiale, in relazione alle norme violate (v. l'art. 83). In termini generali, la soglia inferiore riguarda obblighi strumentali - come ad esempio quelli di documentazione - mentre la soglia superiore è applicabile alla violazione di obblighi finali, di tutela immediata degli interessati.

(19) Si v. diffusamente M. Macchia, C. Figliolia, *Autorità per la privacy e Comitato europeo nel quadro del General Data Protection Regulation*, in questo stesso fascicolo, *infra*, 423 ss..

(20) Ancorché non pienamente tale, quantomeno, come si è visto, in relazione ai trattamenti da parte dei soggetti pubblici. V. O. Lynskey, *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press, 2015, 15 ss.

Il Regolamento, da tale punto di vista, è destinato a un'applicazione molto più estesa dei normali sistemi di regolazione, che operano spesso per settori produttivi, e anche di quelli orizzontali che sono legati alla ricorrenza di caratteri del soggetto o dell'attività non così diffusi come il trattamento dei dati personali (21).

Pur con l'unificazione normativa disposta dal GDPR, aspetti rilevanti di tale sistema di regolazione sono rimessi al diritto nazionale. Il Regolamento, ad esempio, disciplina i procedimenti delle autorità di controllo e la tutela in giudizio solo per alcuni principi molto generali (artt. 57-58), rimettendo per il resto ogni scelta alle valutazioni autonome del legislatore interno. Si è visto che il nostro modello originario era stato costruito sull'idea della riservatezza come tutela di diritti individuali ben definiti, con il ricorso al Garante visto essenzialmente come meccanismo alternativo al giudice civile per l'applicazione di tali diritti. Di qui, l'assenza di discipline specifiche per i procedimenti più propriamente di regolazione, il ricorso limitato se non del tutto assente a forme di consultazione e alle analisi d'impatto, la scelta di conservare la giurisdizione ordinaria anche in occasione del D.Lgs. n. 196/2003. Lo spostamento del centro di attenzione sull'*accountability* accentua però la natura amministrativa dei poteri coinvolti e dovrebbe essere accompagnato da adeguate misure di "copertura" procedimentale e giurisdizionale, secondo i tratti tipici delle regolazioni moderne. Inoltre, numerosi meccanismi istituiti dal Regolamento per poter funzionare richiedono regole di supporto nel diritto interno. Si pensi al trattamento dei dati attinenti alle condanne penali e ai reati (art. 10), che interferisce con le attività di molti soggetti pubblici e privati (affidamento di contratti pubblici, modelli ai sensi del decreto n. 231 ecc.) e che il Regolamento consente solo in presenza di un'autorizzazione da parte del diritto interno che "preveda garanzie appropriate per i diritti e le libertà degli interessati". Essendo cessata l'efficacia dell'autorizzazione generale a suo tempo rilasciata dal Garante (22), almeno al momento in cui si scrive la legittimità di trattamenti del genere - pur oggettivamente necessari - potrebbe essere messa in discussione.

L'opera che compete al legislatore nazionale appare in definitiva ancor più complessa e necessaria di quella che ordinariamente discende dal recepimento delle direttive. La legge di delega n. 163/2017 (art. 13) per l'adeguamento al GDPR, ha però un contenuto sommario che sembrerebbe assumere tale adeguamento alla stregua di un "copy out" di una direttiva. La clausola che più potrebbe pesare nell'attuazione della delega (comma 3, lett. d), potrebbe così essere quella che rinviava la disciplina a "specifici provvedimenti attuativi e integrativi adottati dal Garante", con un'amministrativizzazione delle regole solo in parte giustificabile dalla particolarità della materia e dalla difficoltà di anticipare le soluzioni puntuali nella normativa primaria. I primi schemi del decreto delegato che sono stati resi noti, inoltre, si diffondono su aspetti già disciplinati dal Regolamento, scontando verosimilmente una certa imprecisione del criterio di delega sull'abrogazione delle disposizioni del D.Lgs. n. 196/2003 "incompatibili" con il Regolamento (comma 3, lett. a). In realtà, il decreto delegato deve rimuovere ogni disposizione interna che disciplini aspetti normati direttamente dal Regolamento, anche quando la disciplina nazionale sia idealmente coincidente con quella UE. La riproduzione su scala nazionale di una norma del Regolamento UE ne metterebbe difatti in dubbio l'effetto diretto (23). Al contempo, gli schemi di decreto sin qui circolati trascurano vari aspetti che invece, secondo il Regolamento, spetterebbe al diritto nazionale di integrare. Ad esempio, non è sufficiente determinare i fini di interesse pubblico che giustificano i trattamenti dei "dati particolari" ai sensi dell'art. 9, par. 1, lett. g), del Regolamento (come fa l'art. 2 *sexies* che verrebbe inserito nel D.Lgs. n. 196/2003), è necessario anche che la norma faccia emergere la proporzionalità dei trattamenti e preveda misure adeguate di tutela dei diritti degli interessati. Il che, per trattamenti che si intersecano con numerose tipologie di funzioni e attività amministrative, richiederebbe a sua volta una revisione delle molte discipline coinvolte. Sono tutti indici che, al di là del ritardo accumulato, non lasciano ben presagire sulla completezza del quadro regolamentare a venire.

(21) A titolo di esempio, si v. Corte di giustizia, 10 luglio 2018, *Jehovan todistajat*, in causa C-25/17, che ha ritenuto applicabili le norme UE in materia di protezione dei dati personali alle attività di predicazione porta a porta di una comunità religiosa.

(22) L'ultima è stata l'autorizzazione generale n. 7/2016, con termine di efficacia temporale al 25 maggio 2018, coincidente per l'appunto con la data di applicazione del regolamento.

(23) Corte giust. 31 gennaio 1978, *Fratelli Zerbone*, in causa 94/77.