MEDIALAWS
Rivista di diritto dei media
1/2018

La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni

Francesco Pizzetti*

Professore ordinario di Diritto costituzionale,
Università degli Studi di Torino
Già Presidente del Garante per la protezione dei dati personali

La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni

Sommario

Keywords: dati personali, privacy, GDPR, Garante Privacy, direttiva 95/46

1. L'Autorità italiana allo specchio: il bilancio di venti anni.

Il volume "Le nuove frontiere della privacy nelle tecnologie digitali" a cura di Giuseppe Busia, Laura Liguori e Oreste Pollicino, dedicato a celebrare l'attività del Garante per la protezione dei dati italiano nel corso di vent'anni di costante presidio del più moderno tra i diritti fondamentali del cittadino, costituisce innanzitutto una testimonianza del lavoro svolto da un gruppo di donne e di uomini altamente specializzato e fortemente motivato. Sotto la guida di diversi collegi e quattro segretari generali, essi hanno costituito un solido punto di riferimento per diffondere la cultura della tutela della *privacy* in un Paese a questa assai poco sensibile, e per concorrere a "costruire" un diritto fondamentale tanto multiforme quanto, per certi aspetti, persino proteiforme.

Un diritto che, avendo ad oggetto la tutela delle informazioni riferite o riferibili a una persona fisica identificata o identificabile, assume per sua natura aspetti applicativi diversi a seconda del tipo di dati, dei soggetti che pongono in essere i trattamenti, dei rischi che le modalità usate e le finalità per le quali i dati sono trattati possono far correre alla dignità e la libertà delle persone.

Il fatto che tutti i contributi raccolti nel volume siano opera di persone impegnate, da molti anni, in questo sforzo collettivo rende particolarmente interessante quest'opera. Sono, infatti, i protagonisti stessi, molti dei quali presenti in Autorità fin dall'inizio della sua attività, che rendono testimonianza del loro lavoro e del modo col quale esso è stato ed è svolto.

Queste pagine sono, dunque, anche la testimonianza di una esperienza di vita e di una

[*] Il presente contributo è precedentemente comparso come prefazione al volume G. Busia – L. Liguori – O. Pollicino (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali: bilanci e prospettive*, Roma, 2016, pubblicato in occasione del ventennale del Garante per la protezione dei dati personali.

passione che va ben oltre una normale attività lavorativa. Da esse emerge con chiarezza che gli autori di questi scritti, e tutti i loro colleghi, hanno in comune la consapevolezza che il loro lavoro è una difesa importante della convivenza democratica e dei diritti fondamentali delle persone. Un presidio di libertà tanto più necessario oggi, di fronte all' esplosione della società digitale e di tecnologie che, grazie alla interconnessione sempre più massiva e veloce dei dati, aprono continuamente scenari nuovi, ricchi di promesse ma anche di pericoli.
Già questo basterebbe per affermare che questo volume merita di figurare nella biblioteca di chiunque voglia occuparsi di questa materia.

2. L'Autorità italiana e il legislatore nazionale di fronte alla sfida del futuro

Sarebbe, però, molto riduttivo limitarsi a considerare gli scritti raccolti nel volume come un bilancio, sia pure ampio e importante, dell'attività svolta in questi venti anni. Tutti i contenuti raccolti si misurano, infatti, non solo col passato o col presente ma anche, e soprattutto, col futuro.
Questo vale in primo luogo per quelli, e sono numerosi, che si misurano col nuovo regolamento e con le innovazioni che esso comporta.
Dalla riflessione sul concetto di dato e delle tecniche di trattamento che il nuovo regolamento introduce, all'analisi sul consenso informato e sulle nuove regole relative al trasferimento dei dati all'estero, fino al lungo saggio dedicato al ruolo delle Autorità di controllo, vi sono nel volume contributi che dimostrano quanto ampia sia l'attenzione del Garante in questo periodo di transizione tra la direttiva, tuttora vigente, e il regolamento, anch'esso già in vigore, ma destinato a trovare piena attuazione soltanto dal 25 maggio 2018.
Alcuni di questi contributi appaiono più attenti alla valorizzazione della storia dell'Autorità e alla difesa della compatibilità tra legislazione nazionale e nuovi scenari europei, altri sono invece più interessati alle sfide del domani.
Si tratta, però, sempre di riflessioni che testimoniano l'attenzione con la quale, come è sempre stato nel passato, ancor più oggi viene seguito il dibattito a livello europeo e il notevole contributo che l'Autorità italiana sta dando al lavoro collettivo in atto nell'ambito del Gruppo di lavoro Articolo 29. Un impegno pesante e prezioso ma certamente molto importante soprattutto nella fase attuale, in cui il nuovo regolamento è già in vigore ma non avrà piena attuazione fino al 25 maggio del 2018.
Occorre, infatti, predisporre linee guida e provvedimenti chiarificatori di molti aspetti centrali nel sistema della nuova normativa, in modo da evitare che la transizione dal vecchio al nuovo ordinamento possa lasciare anche solo per breve tempo parzialmente scoperta o incerta la protezione dei dati personali dei cittadini europei.
Ancora più importante, poi, adeguare le Autorità nazionali ai loro nuovi, molto più ampi, compiti, e al lavoro comune che, sia nell'ambito dei meccanismi di coerenza che del nuovo Gruppo di protezione dei dati, sono chiamate a svolgere.
Infine occorre che il legislatore nazionale avvii rapidamente una riflessione approfon-

dita sulle modifiche da apportare alla legislazione nazionale, sia per colmare le lacune di quella europea, sia per compiere le scelte e sciogliere i nodi che volutamente il regolamento lascia alla legislazione degli Stati.

Merita ricordare sempre, infatti, che la protezione dei dati personali ha una assoluta centralità nell'Unione Europea, specialmente da quando, con l'entrata in vigore del Trattato di Lisbona, è stata riconosciuta come diritto fondamentale dell'Unione, secondo quanto stabilito dall'art. 8 della Carta dei diritti fondamentali dell'Unione e dall'art. 16 del TFUE. Essa deve dunque essere sempre tutelata al massimo livello, e senza pericolose fasi di incertezza, in tutto il territorio dell'Unione e rispetto a ognuno dei suoi cittadini.

Non meno importanti sono i contributi relativi a settori nei quali la normativa italiana del Codice della Privacy, anche dopo il necessario adeguamento del legislatore nazionale al nuovo quadro normativo, è probabilmente destinata a restare ancora a lungo centrale.

Tuttavia, come sarà più ampiamente descritto nei paragrafi successivi in numerosi e strategici settori, è il regolamento stesso che rimette gran parte della regolazione alla legislazione degli Stati.

Anche in questi settori, dunque, è necessario essere attentissimi a guardare oltre l'esperienza passata e presente. È importante essere consapevoli, infatti, che la legislazione nazionale dovrà essere comunque applicata in modo coerente coi principi del nuovo regolamento, anche se ciò potrà richiedere interventi normativi innovativi rispetto al Codice attuale.

Il *corpus iuris* prodotto dal Garante in questi venti anni mantiene tuttavia una validità indiscutibile, che potrà orientare anche l'applicazione del nuovo regolamento.

Questo vale, in particolare, per le parti relative alla sanità, ai rapporti di lavoro, all'informazione e alla stampa, alla giustizia e alla sicurezza.

Un discorso a sé merita invece la parte relativa alla comunicazione istituzionale. Si tratta di un contributo molto interessante che sottolinea l'attenzione con la quale, in questo ventennio, è stato svolto uno dei compiti principali dell'Autorità: quello relativo alla diffusione della cultura della protezione dei dati personali. Affrontando il bilancio di questi venti anni tema dal punto di vista della comunicazione va anche messo in rilievo lo sviluppo di alcune prassi, come ad esempio la redazioni di Linee Guida, che la Autorità italiana ha adottato a partire dalla seconda metà degli anni duemila, malgrado non poche resistenze anche al suo interno. Si tratta di una tipologia di provvedimenti divenuta ora anche oggetto della nuova normativa europea, che considera proprio la redazione delle Linee Guida fra i compiti del Gruppo europeo di protezione dei dati personali[1].

Infine, dal contributo sulla comunicazione emerge con nettezza il profilo di una Autorità consapevole che una comunicazione adeguata ai tempi deve presidiare non solo i media tradizionali e quelli *online*, ma anche i *social* e i *blog* dedicati, e deve essere pronta a utilizzare ogni mezzo che possa aiutare a diffondere la conoscenza dei valori in gioco: dagli opuscoli esplicativi per i giovani e le famiglie, ai concorsi nelle scuole; dalle pub-

[1] Cfr. regolamento 2016/679, art. 70, par. 1, lettere *d), f), h), i), j), m).*

blicazioni per gli operatori dei vari settori all'organizzazione di dibattiti e occasioni di approfondimento con i cultori delle diverse discipline interessate.

3. Un osservatorio privilegiato per il futuro

Siamo dunque di fronte a una raccolta di scritti importante anche, e soprattutto, perché consente di comprendere come chi guarda al futuro da un osservatorio privilegiato si figura i problemi più importanti dei prossimi anni. Un aiuto utilissimo per chiunque voglia comprendere i nuovi scenari della protezione dei dati personali.
Cercando di dare un ulteriore contributo allo sforzo collettivo che costituisce il pregio maggiore di questa raccolta, si possono fissare alcuni grandi capisaldi che caratterizzano la nuova regolazione e segnano, nel loro insieme, il grande salto di qualità dell'Unione Europea in materia di protezione dei dati personali.
Al centro della scena vi è innanzitutto la transizione dalla direttiva al regolamento e l'urgenza di mettere a fuoco gli aspetti più innovativi della nuova disciplina.
Fra le innovazioni di maggiore interesse va segnalato certamente il profondo cambiamento del ruolo delle Autorità. Non meno importante, però, è la centralità che assumono il titolare e il responsabile del trattamento. Sia pure in misura diversa fra loro, su queste figure ricade ora la responsabilità di verificare innanzitutto che i trattamenti posti in essere siano, sin dalla loro progettazione e dalle modalità adottate per svolgerli, conformi al livello di rischio che comportano. Una valutazione che incide anche direttamente sulle misure di sicurezza da adottare a seconda dei casi e dei rischi che possono correre i diritti e le libertà degli interessati.
Accanto alle accresciute responsabilità dei titolari e dei responsabili, si collocano anche le nuove garanzie assicurate agli interessati.
La *privacy by design*, la *privacy by default*; il ricorso alla pseudoanonimizzazone come misura di garanzia e allo stesso tempo di sicurezza; l'obbligo di valutare, anche in dialogo con le Autorità, l'impatto dei trattamenti sulla tutela dei dati personali quando si utilizzino le nuove tecnologie; l'obbligo di denuncia delle *data breaches* per ogni settore produttivo e per ogni articolazione della pubblica amministrazione; l'obbligo di adottare misure di sicurezza adeguate ai rischi dei trattamenti, specialmente con riguardo alla perdita, modifica, divulgazione non autorizzata o accesso in modo illegale o accidentale ai dati; l'obbligo o l'opportunità di nominare il *Data Protection Officer*: questi e molti altri ancora sono i punti cardinali che definiscono allo stesso tempo le accresciute responsabilità di chi pone in opera i trattamenti e le nuove garanzie assicurate a coloro a cui dati trattati appartengono.
Agli interessati, che restano ovviamente figure centrali anche nel nuovo regolamento, sono riconosciuti, accanto a quelli tradizionali, anche nuovi diritti quali la portabilità dei dati, il diritto a una cancellazione "rafforzata" (diritto all'oblio), il diritto alla limitazione dei trattamenti, l'obbligo per il titolare di notificare ai destinatari, a cui sono stati trasmessi, l'eventuale rettifica o cancellazione dei dati o la limitazione dei trattamenti.
A questi diritti, in larga parte nuovi nel contenuto e nelle modalità di attuazione, si ag-

giungono anche le rafforzate garanzie relative ai trasferimenti di dati all'estero.

4. Il nuovo regolamento: una normativa flessibile che guarda al futuro e alle nuove tecnologie

Bastano questi rapidi cenni per comprendere che l'obiettivo principale del regolamento è assicurare la protezione dei dati personali attraverso un quadro normativo adeguato a misurarsi con le nuove tecnologie dell'informazione e le nuove e più complesse esigenze della società in cui viviamo.
Al medesimo tempo la nuova normativa, consapevole di dover presidiare e tutelare un diritto che, per sua natura, è continuamente messo a rischio dalla continua evoluzione della società digitale e delle sue tecnologie, contiene anche strumenti di flessibilità estremamente importanti, che chiamano in causa direttamente le Autorità.
Senza pretesa di esaustività, possiamo ricordare tra i principali: la già citata valutazione di impatto, obbligatoria quando i trattamenti comportino l'uso di nuove tecnologie che mettono a rischio la libertà e i diritti delle persone fisiche, e il connesso obbligo di consultare le Autorità quando il rischio del trattamento appaia elevato; la possibilità per Stati membri e Autorità di controllo di prevedere meccanismi di certificazione nonché sigilli e marchi di protezione, insieme ad adeguati organismi di certificazione; la approvazione di codici di condotta predisposti in funzione delle specificità dei diversi settori e delle esigenze delle micro, piccole e medie imprese; il monitoraggio costante dei codici di condotta approvati.
Alle Autorità di controllo spetta inoltre non solo sorvegliare e vigilare sull'applicazione del regolamento ma anche promuovere la consapevolezza e la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione ai trattamenti.
A questi obblighi si aggiungono quello di fornire consulenza al Parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative da adottare, nonché quello di promuovere la consapevolezza dei titolari e dei responsabili del trattamento riguardo agli obblighi a loro imposti dal regolamento, ovviamente valutati con riferimento alle caratteristiche, anche tecnologiche, dei trattamenti concretamente posti in essere.
In questo quadro sarebbe dunque profondamente sbagliato leggere i nuovi doveri dei titolari e dei responsabili, i diritti degli interessati e i nuovi poteri e compiti delle Autorità in una dimensione tendenzialmente statica, che vede la realtà come immutabile, come per molto tempo si è fatto nell'ambito della direttiva.

5. La nuova centralità dei titolari e dei responsabili e il rapporto con le Autorità

La scelta fatta dal regolamento di "caricare" sui titolari e i responsabili il dovere di adottare in via preventiva misure idonee a garantire la protezione dei dati personali,

nonché l'obbligo di valutare essi stessi, in rapporto ai rischi dei trattamenti, quali misure di sicurezza debbano essere adottate, ha un chiarissimo significato di carattere sistemico. Essa dimostra che si è voluto predisporre un quadro normativo aperto al futuro e adeguato a dare tutela a una grande pluralità di trattamenti possibili, anche in previsione delle nuove inevitabili evoluzioni che la tecnologia digitale avrà in questa materia. È solo in questo quadro che diventa comprensibile perché si sia rimesso ai titolari e ai responsabili il compito di valutare essi stessi, talvolta in colloquio con l'Autorità, il livello di rischio, e conseguentemente le misure di sicurezza da garantire; fermo restando comunque l'obbligo di adottare fin dall'inizio dei trattamenti modalità e misure tecniche adeguate ad assicurare una protezione preventiva, e in qualche modo automatica, dei dati personali.

Coerentemente con questa impostazione, anche il ruolo delle Autorità di controllo non può più essere visto in modo sostanzialmente statico, come un compito di vigilanza e controllo sulle attività dei titolari e i trattamenti posti in essere, finalizzato essenzialmente a dare tutela all'interessato, in particolare quando questi che ne faccia richiesta.

Nel quadro del nuovo regolamento il ruolo delle Autorità è strutturalmente dinamico sia nei confronti dei titolari che dei regolatori pubblici. Non solo: oggetto ultimo della tutela che spetta alle Autorità assicurare non sono più soltanto i diritti dei singoli interessati ma anche quelli della società nel suo complesso.

Rispetto al rapporto tra Autorità e titolari, assume un rilievo centrale la possibilità, nella direttiva assai meno enfatizzata (cfr. art. 28, comma 3, direttiva 95/46/CE), di prevedere meccanismi di certificazione e codici etici, così come il coinvolgimento necessario delle Autorità nella valutazione di impatto sui trattamenti che comportino l'uso di nuove tecnologie e presentino rischi elevati in assenza di adeguate misure che possano attenuarli (art. 36).

Non meno significativo rispetto al nuovo ruolo assegnato alle Autorità è quello previsto dall'art. 57, paragrafo primo, lett. *b)* relativo alla promozione della consapevolezza e della comprensione del pubblico «riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione ai trattamenti». Si tratta di un compito che nell'ambito della direttiva non è esplicitamente previsto e che, invece, nel nuovo contesto assume un rilievo estremamente importante.

Esso conferma in modo chiarissimo che il regolamento si colloca in una prospettiva "dinamica", che vede la tutela della protezione dei dati personali non solo come un diritto fondamentale dei cittadini ma anche come un valore sociale di diritto pubblico europeo.

È ovvio che in una società digitale, in continuo mutamento anche rispetto alle tecnologie adottate, i trattamenti possono variare a seconda dei casi, delle finalità, delle innovazioni sviluppate. Promuovere la consapevolezza e la comprensione di questi fenomeni, e delle norme e diritti specificamente coinvolti, significa dunque assicurare che il pubblico (e cioè la società nel suo complesso) sia costantemente messo in grado di comprendere anche i rischi che l'evoluzione delle tecnologie e dei connessi trattamenti di dati possono comportare.

L'obbligo di individuare e promuovere la conoscenza delle garanzie e delle norme

applicabili, necessariamente connesso anche all'evoluzione dei trattamenti, completa il salto di qualità che il nuovo regolamento fa oggettivamente fare alle Autorità.

6. Il nuovo ruolo delle Autorità

Proprio l'art. 57, paragrafo primo, lett. *b)* è la norma che più di ogni altra dimostra la consapevolezza dell'esistenza di tre fenomeni tra loro correlati, che concorrono tutti a dare alle Autorità un ruolo molto più incisivo e importante del passato.
Il primo fenomeno è legato all'inarrestabile sviluppo della società digitale e dei trattamenti di dati in continuo aumento e mutamento. Ciò richiede Autorità capaci di seguire costantemente i processi tecnologici; di valutarne le conseguenze sull'uso dei dati personali; di assicurare una costante informazione sulle conseguenze che le nuove tecnologie, e i trattamenti che comportano, possono presentare per tutta la comunità nazionale di riferimento.
Il secondo fenomeno è connesso alla necessità di prestare specifica attenzione alle conseguenze che gli sviluppi delle nuove tecnologie, pur in una società globalizzata, e tendenzialmente tutta interconnessa, possono avere nella realtà nazionale.
La differenza di incidenza specifica relativa a ciascun Paese può avere molte cause: dall'ampiezza di banda alla diffusione delle reti di interconnessione sul territorio; dai tipi di *device* maggiormente diffusi e utilizzati, alle caratteristiche socio-economiche nei diversi Paesi; dalla conoscenza e applicazione delle tecnologie nei diversi settori pubblici e privati alla capacità degli utenti di saper utilizzare i servizi *online*. Inoltre, l'integrazione dei sistemi digitali e delle reti di telecomunicazioni è ancora molto frammentata, anche nell'ambito dell'UE, e non siamo vicini a un reale Mercato Unico Digitale.
Di qui la spiegazione del perché il compito di informare costantemente il pubblico delle evoluzioni in atto e dei rischi che i diversi trattamenti possono presentare, oltre che delle norme da applicare e le garanzie da invocare, sia affidato dal regolamento alle Autorità nazionali.
Sottesa a questa disposizione vi è, insomma, la consapevolezza che, per quanto tendenzialmente globalizzata, la società digitale ha ancora dimensioni nazionali, e persino territoriali, diverse. Ovviamente questo non scalfisce in nulla l'impegno del regolamento a garantire che, anche grazie alla stretta collaborazione fra le Autorità, sia nella realtà nazionale che nel contesto europeo sia assicurata sostanziale uniformità di regolazione e omogeneità di principi. Proprio questo, però, esalta il ruolo delle Autorità. Solo queste, infatti, operando nell'ambito dei meccanismi di cooperazione e di coerenza e lavorando insieme nel Gruppo europeo di protezione dati, possono garantire che il necessario rispetto delle differenze tra le diverse comunità non conduca mai a forme di *digital*, *cultural*, *economic divide* tra i diversi Paesi, inaccettabili in una Unione strettamente interconnessa e immersa nella realtà globale della nostra epoca.
L'obbiettivo da raggiungere, infatti, è diffondere la conoscenza dei rischi che la società digitale comporta per le persone ma, allo stesso tempo, assicurare la possibilità di cogliere le infinite opportunità che lo sviluppo della tecnologia offre per lo sviluppo della

persona umana e per le sue potenzialità di vita e di crescita.
In questo quadro l'attenzione al contesto dei singoli Paesi è un aspetto che arricchisce ulteriormente il significato del nuovo regolamento. Essa, del resto, è confermata anche dalla lett. *c)* del medesimo paragrafo primo dell'art. 57, secondo il quale le Autorità di controllo devono prestare costante consulenza e supporto ai Parlamenti e ai regolatori nazionali oltre che alla autorità amministrative del proprio Paese. Una evidente conferma della consapevolezza che anche la regolazione nazionale deve tener conto delle specificità nazionali, specialmente con riferimento allo sviluppo digitale di ciascun Paese.
Il terzo, e più importante, fenomeno che sottostà a queste norme è la consapevolezza che, pur restando legata alla tutela di un diritto fondamentale dell'individuo, la protezione dei dati, *anche personali*[2], è diventata una esigenza di interesse pubblico che riguarda l'intera società. Per questo essa deve essere presidiata non solo a tutela dell'interessato e a sua richiesta ma anche in via generale e preventiva.
Questa visione del concetto di protezione dei dati personali come interesse generale si trova in modo molto limitato nella direttiva. Solo in due punti, infatti, essa individua un ruolo delle Autorità di controllo che si estende oltre la tutela dell'interessato e riguarda anche aspetti di carattere generale.

[2] Il corsivo sottolinea la convinzione di chi scrive che nel mondo di oggi, e ancor più in quello di domani, la protezione dei dati sia sempre più vitale per le relazioni sociali, economiche e politiche che caratterizzano le nostre società e, in particolare con riguardo alla libertà di informazione, comunicazione e pensiero, anche la nostra convivenza democratica. Di conseguenza è sempre più importante fare tesoro dell'esperienza accumulata nell'attività di tutela dei dati personali per estenderla, *mutatis mutandis*, anche ai trattamenti di dati *tout court*, indipendentemente dal fatto che contengano informazioni riconducibili a una persona identificata o identificabile. Di qui la convinzione che tanto il ruolo delle Autorità di controllo quanto quello degli studiosi che si occupano, sia sotto il profilo giuridico che tecnico, della tutela dei dati personali, debba sempre più estendersi anche a esplorare i temi connessi alla protezione dei dati e dei loro trattamenti, anche quanto concernano attività più direttamente legate alla c.d. Internet delle cose o a forme di Intelligenza Artificiale basate sull'analisi di dati anonimi o comunque non riferibili a persone. Sulla tematica della protezione dei dati personali tra diritto fondamentale della persona e principio di interesse pubblico europeo si vedano i diversi spunti contenuti *passim* in F. Pizzetti, *Privacy e il diritto europea alla protezione dei dati personali*, vol. I, *Dalla Direttiva 95/46 al nuovo Regolamento europeo*, e Id. *Privacy e diritto europeo alla protezione dei dati personali*, vol. II, *Il Regolamento europeo 2016/679*, Torino, 2016. Sull'intreccio tra regolamento, tutela dei dati personali e tematica generale relativa ai trattamenti dati cfr. G. D'Acquisto - M. Naldi, *Big Data e Privacy by design. Anonimizzazione, Pseudoanonimizzazione, Sicurezza*, Torino, 2017.

Il primo caso riguarda il dovere di notificazione dei trattamenti alle Autorità nazionali[3], una misura che è stata vissuta in modo burocratico, e anche per questo abolita dal regolamento, ma che nelle intenzioni del regolatore del 1995 aveva lo scopo di assicurare che vi fosse in ogni Paese un "custode" dei registri dei trattamenti posti in essere nel territorio nazionale. Il secondo caso è la norma che impone al Gruppo di lavoro Articolo 29 di collaborare, anche in modo propositivo, con la Commissione[4].
Anche nella Carta dei diritti e nel TFUE la tutela dei dati personali è considerata es-

[3] La direttiva dedica ben due articoli, il 18 e il 19, all'obbligo di notificazione dei trattamenti e al contenuto di tale obbligo. È certamente questo il punto in cui la direttiva assegna alle Autorità un importante ruolo di carattere generale e di evidente interesse pubblico, quale la tenuta dei registri dei trattamenti. Questo aspetto è particolarmente interessante perché segna bene il mutamento di prospettiva tra i due sistemi normativi. Infatti, in coerenza con la consapevolezza che pervade tutto il regolamento relativamente al continuo sviluppo delle tecnologie relative all'utilizzazione dei dati e ai relativi trattamenti, il nuovo quadro normativo pone ora a carico dei titolari il compito di tenere i registri dei trattamenti effettuati. A prima vista può apparire una contraddizione inspiegabile fra una direttiva che, pur ispirata alla centralità della tutela del diritto individuale, ha posto però a carico dell'Autorità il compito di tenere i registri dei trattamenti, e un regolamento che, pur dando rilievo all'interesse generale alla tutela dei dati personali, pone invece a carico dei titolari l'obbligo di tenere i registri dei trattamenti effettuati. In realtà non siamo di fronte a una contraddizione ma, al contrario, alla conseguenza logica della diversa impostazione dei due contesti normativi. La direttiva è stata strutturata su una visione sostanzialmente statica delle tipologie dei trattamenti e della tutela da garantire. Al contrario, il regolamento è incentrato su una visione dinamica, che sconta continue evoluzioni e una crescita esponenziale dell'uso dei dati. Di qui la diversa impostazione del regime relativo ai registri di trattamenti e la coerenza delle ragioni della differente disciplina

[4] Merita ricordare infatti che l'art. 30 della direttiva 95/46/CE assegna al Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali tra gli altri compiti anche quello di «formulare, ad uso della Commissione, un parere sul livello di tutela nella Comunità e nei paesi terzi» (cfr. art. 30, par. 1, lett. *b*) e quello di «consigliare la Commissione in merito ad ogni progetto di modifica della presente direttiva, ogni progetto di misure addizionali o specifiche da prendere ai fini della tutela dei diritti e delle libertà delle persone fisiche con riguardo a qualsiasi progetto di misure comunitarie che incidano su tali diritti e libertà» (cfr. art. 30, par. 1, lett. *c*).

senzialmente come un diritto fondamentale della persona[5], con la conseguenza che il ruolo delle Autorità, pur richiamato nelle norme, è strettamente connesso alla effettività del diritto del singolo interessato.
Il ruolo delle Autorità di controllo si amplia invece, con forza persino inattesa, nel nuovo regolamento che fa di esse, e dei compiti di interesse generale che sono chiamate ad assolvere, uno dei tratti più interessanti della nuova normativa.
Allo stesso tempo, proprio il ruolo ampliato delle Autorità costituisce, insieme alla centralità assunta dalla responsabilità del titolare, un indicatore evidente che il regolamento stesso, pur avendo la sua base normativa nel Trattato e nel riconoscimento della protezione dei dati personali come diritto fondamentale, va molto oltre e guarda molto più lontano di una mera tutela giuridica dell'interessato, da far valere nell'ambito di un contenzioso davanti a una Autorità o a un giudice.

7. Il diritto alla protezione dei dati personali come diritto pubblico europeo e l'evoluzione delle Autorità

Gli aspetti che testimoniano questa evoluzione sono numerosi.
Si pensi, ad esempio, al dovere del titolare del trattamento di denunciare all'Autorità di controllo, senza ingiustificato ritardo e comunque entro termini brevi, specificamente stabiliti, ogni violazione di dati (*data breaches*) che si sia verificata, per il fatto stesso che ciò sia avvenuto. Un obbligo al quale il titolare può sottrarsi solo se ritiene, assumendosene la responsabilità, che sia «improbabile che la violazione dei dati personali presenti

[5] Cfr. Carta dei diritti fondamentali dell'Unione, art. 8, terzo paragrafo: «Il rispetto delle regole è soggetto al controllo di un'autorità indipendente». Non diversamente l'art. 16 del TFUE stabilisce alla fine del secondo paragrafo: «Il rispetto di tali norme è soggetto al controllo di autorità indipendenti». Merita ricordare tuttavia che l'art. 8 della Carta dei diritti dell'Unione Europea adottata dal Trattato di Lisbona non si limita a stabilire al primo paragrafo che «Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano». Al secondo paragrafo, infatti, la disposizione specifica anche che «Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o altro fondamento previsto dalla legge. Ogni persona ha il diritto di accedere ai dati che la riguardano e di ottenerne la rettifica». È pacifico che la disposizione citata richiama e precisa i principi tradizionali della protezione dei dati personali, come messi a fuoco dalla Convenzione 108, prima, dalla direttiva 95/46, dopo. Tuttavia è evidente che essa sottolinea con forza il richiamo al principio di lealtà e di finalità determinate. Principi, questi, certamente essenziali quando i dati sono trattati sulla base del consenso ma che, non a caso, la disposizione, in coerenza con la direttiva, ricollega anche ai casi in cui i dati siano trattati sulla base di un altro fondamento legittimo previsto dalla legge. In questo senso la Carta dei diritti eleva a principi fondamentali anche il principio di lealtà dei trattamenti e di determinatezza delle finalità per le quali essi sono posti in essere. Si tratta di principi che possono e devono valere per qualunque trattamento di dati.
Più generico invece l'art. 16 del TFUE che riguarda solo i trattamenti dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione nonché quelli degli Stati membri nell'esercizio di attività che rientrino nell'campo di applicazione del diritto dell'Unione e si limita a rinviare a norme da adottare, secondo la procedura legislativa ordinaria, dal Parlamento e dal Consiglio. Merita sottolineare inoltre che la normativa alla quale fa riferimento l'art. 16 del TFUE si concretizza oggi soprattutto nel regolamento 2016/679 oltre che, per le attività di polizia, giustizia e sicurezza, nella direttiva 2016/680. Di conseguenza poiché, come si sottolinea nel testo, il regolamento è ispirato a una visione più ampia della semplice tutela del diritto fondamentale alla protezione dei dati personali, aprendo la strada anche alla tutela dei dati come valore sociale, è giusto dire che è proprio il Trattato sul funzionamento dell'Unione che, con la sua voluta genericità, ha posto le premesse per questa evoluzione.

un rischio per i diritti e le libertà delle persone fisiche».
Per contro, l'art. 34 stabilisce invece che il titolare è tenuto a comunicare all'interessato le eventuali violazioni di suoi dati personali solo se, sempre sotto la sua responsabilità, valuta che le perdite possono determinare rischi elevati per la persona, o se è l'Autorità stessa che lo impone.
È del tutto evidente che la diversità di disciplina massimizza il ruolo dell'Autorità di controllo a tutela dell'interesse generale a che le violazioni non si verifichino o, ove ciò avvenga, si adottino le misure necessarie per impedirne il ripetersi. Se invece il regolamento fosse rimasto strettamente legato alla sola, o prevalente, prospettiva della tutela del diritto fondamentale della persona, è chiaro che l'obbligo di comunicazione e notifica avrebbe dovuto riguardare sempre e prima di tutto l'interessato.
Insomma, in una visione che avesse continuato a considerare centrale sempre e comunque la tutela del diritto dell'interessato, la disciplina relativa all'obbligo di denuncia delle violazioni (*data breaches*) avrebbe dovuto essere esattamente rovesciata.
Molte altre disposizioni possono essere richiamate per dimostrare come il regolamento abbia voluto dichiaratamente affidare alle Autorità di controllo compiti che vanno molto oltre la verifica e la sorveglianza circa la corretta attuazione della normativa e la tutela degli interessati.
Si pensi ai compiti assegnati dall'art. 41 alle Autorità per quanto riguarda il monitoraggio sui codici di condotta e la definizione dei criteri per l'accreditamento degli organismi relativi.
Si pensi ai compiti e ai poteri assegnati alle Autorità dall'art. 42 in materia di certificazioni, marchi e sigilli.
Si pensi al ruolo assegnato dagli artt. 35 e 36 alle Autorità nell'ambito delle valutazioni di impatto, specialmente quando i trattamenti comportino l'uso di nuove tecnologie che possano comportare rischi elevati per i diritti e le libertà delle persone. In questo ambito, inoltre, merita una attenzione particolare il paragrafo quinto dell'art. 36, che consente agli Stati membri di prevedere non solo la consultazione obbligatoria delle Autorità ma anche la loro specifica autorizzazione rispetto a trattamenti posti in essere «per l'esecuzione, da parte del titolare, di un compito di interesse pubblico», tra i quali sono specificamente indicati quelli in materia di protezione sociale e di sanità pubblica.
Si potrebbero richiamare molte altre norme e fare ulteriori esempi ma, *last but non least*, almeno uno fra gli ulteriori compiti e poteri assegnati alle Autorità di controllo merita una sottolineatura particolare. Si tratta di quanto previsto dalla lett. *i)* del primo paragrafo dell'art. 57, laddove si stabilisce che ciascuna Autorità «sorveglia gli sviluppi che presentano un interesse, se e in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione e le prassi commerciali». Ciò che colpisce particolarmente è che le Autorità sono chiamate a svolgere questo compito in via generale e preventiva, per il solo fatto che determinati sviluppi, specialmente (ma non unicamente) nei settori indicati, possano incidere sulla protezione dei dati personali. Si tratta di garantire un monitoraggio continuo sugli aspetti più delicati dell'evoluzione della società digitale e dell'innovazione tecnologica, indipendentemente dal fatto che siano o meno in atto trattamenti concreti di dati rela-

tivi a persone fisiche interessate.

8. Dalla direttiva 95/46/CE al regolamento: dal mondo di ieri a quello di domani

Non sembrano esservi dunque dubbi sul fatto che il nuovo regolamento, pur mantenendo sostanzialmente fermi i concetti tradizionali fra i quali in particolare quelli cardinali, relativi alle nozioni di dato, di trattamento, di interessato, di titolare, di responsabile, si colloca in una visione del tutto diversa da quella della direttiva, segnando anche concretamente gli enormi mutamenti intervenuti in questa materia durante i venti anni trascorsi tra i due strumenti normativi.

Tanto la direttiva è stata caratterizzata da una struttura rigida e da una concezione sostanzialmente statica della protezione dei dati personali, tanto il regolamento ha alla sua base una concezione normativa dinamica e flessibile, che sconta una continua e inevitabile evoluzione di un settore così strategico nell'ambito della società digitale.

Mentre la direttiva ha posto al centro della sua normativa il dato personale, le condizioni da rispettare per la liceità dei trattamenti e i diritti dell'interessato, il regolamento è strutturalmente incentrato sul titolare e la sua responsabilità. Una responsabilità che è sempre commisurata ai rischi che i trattamenti posti in essere possono determinare, e la cui valutazione, dalla quale dipende anche l'individuazione delle misure di sicurezza da adottare, è sempre rimessa al titolare.

In questo quadro, sia la posizione dell'interessato che la tutela dei suoi diritti, pur restando formalmente centrali, finiscono per essere collocati sullo sfondo, mentre emerge in tutta la sua forza la valutazione di impatto dei trattamenti che spetta al titolare fare e dalla quale dipendono anche le condizioni che devono esser soddisfatte affinché il trattamento sia lecito e conforme alla normativa.

Infine, mentre nel quadro della direttiva l'Autorità era chiamata a svolgere soprattutto un ruolo di garanzia, focalizzato sulla tutela dei diritti dell'interessato e sull'adozione delle misure necessarie ad assicurare che essi fossero rispettati e difesi, tanto nel regolamento l'Autorità diventa presidio della legittimità dei trattamenti e del rispetto del corretto uso dei dati nell'ambito di società digitale in continua evoluzione. Per questo spetta ad essa anche un monitoraggio continuo sulle innovazioni che possono comportare rischi crescenti non solo per le persone fisiche di volta in volta interessate, ma anche per tutta la comunità.

A questo va aggiunto che, attraverso i meccanismi di cooperazione e coerenza e la partecipazione al Gruppo europeo di protezione dei dati personali, i cui poteri sono enormemente cresciuti rispetto al Gruppo art. 29 previsto dalla direttiva, le Autorità nazionali sono chiamate anche a essere presidio e tutela della società europea nel suo complesso.

9. Due errori da evitare nell'analisi del nuovo regolamento e del ruolo delle Autorità

Basterebbero già queste considerazioni per sottolineare l'enorme cambiamento in atto che impone anche all'Autorità italiana, come a quelle degli altri Paesi, di prepararsi a sfide e compiti molto più importanti e strategici di quelli, pur molto rilevanti, che ha svolto finora.

Il ruolo delle Autorità, come tutta la materia relativa alla protezione dei dati personali assume un aspetto ancora più rilevante se si tiene conto che il nuovo regolamento, proprio perché ha l'obiettivo di assicurare, almeno entro certi limiti, una tutela uniforme su tutto il territorio europeo, è costretto a non limitarsi a imporre norme rigide e rigidamente applicabili in ogni campo ma a fare i conti, invece, con forti elementi di flessibilità.

Del resto, finora i commentatori hanno prestato attenzione soprattutto a sottolineare il salto di qualità connesso al passaggio da una direttiva di armonizzazione, che scontava leggi nazionali diverse tra loro anche se vincolate al rispetto di principi, criteri e condizioni comuni, a una fonte come il regolamento, di per sé vincolante e immediatamente applicabile in tutti gli Stati membri.

Si è, inoltre, visto in questo mutamento di scenario l'effetto di una scelta imposta dal riconoscimento del diritto alla protezione dei dati personali come diritto fondamentale dell'Unione contenuto nella Carta dei diritti e nel Trattato di Lisbona. Secondo questa impostazione, infatti, ciò ha reso indispensabile l'adozione di una regolazione uniforme che fosse in grado di assicurare le medesime garanzie a tutti i cittadini europei.

Questa "lettura" del regolamento è indiscutibilmente fondata e condivisibile.

Del resto è questo il quadro nel quale la nuova normativa è stata presentata fin da quando la Commissione europea promosse, nel lontano luglio 2009, la *Consultation on the legal framework for the fundamental right to protection of personal data*[6]. Fu infatti da quella Consultazione che scaturirono le prime indicazioni che condussero poi alla presentazione da parte della Commissione, il 1 gennaio 2012, della proposta che è alla base dell'attuale regolamento 2016/679.

In particolare, proprio da quella Consultazione e, soprattutto, dal successivo Parere del Gruppo di lavoro Articolo 29 sul Futuro della Privacy[7], scaturirono le considerazioni che sono poi state alla base dell'attenzione dedicata al ruolo delle Autorità.

È in questo quadro che vanno collocati gli strumenti di cooperazione e coerenza previsti dal nuovo regolamento; i poteri, compiti e modalità di procedere dell'Autorità capofila; il meccanismo di coerenza di cui alla sezione II del Capo VII. Di qui, infine, il ruolo, forte e robustamente costruito, assegnato al nuovo Comitato europeo per la protezione dei dati personali di cui alla Sezione terza del medesimo Capo VII.

---

[6] Il Gruppo di lavoro Articolo 29 produsse, in risposta alla Consultazione della Commissione, una importante *Opinion*, che conteneva già i capisaldi di quella che sarebbe poi diventata la proposta di regolamento presentata dalla Commissione. Cfr. Gruppo di lavoro Articolo 29, *Opinion on the future of privacy*, 1°dicembre 2009, WP168

[7] Cfr. Gruppo di lavoro Articolo 29, WP168, cit. alla nota precedente

Tutto questo riconosciuto e ribadito, merita tuttavia sottolineare che vi sono almeno due errori che è bene evitare, tanto nell'analisi del regolamento quanto, e soprattutto, nella riflessione sul ruolo delle Autorità di controllo e della protezione dei dati personali nell'ambito dell'Unione.

Il primo riguarda una possibile eccessiva sopravvalutazione degli elementi unificanti contenuti nel regolamento.

In realtà la "flessibilità" della nuova normativa non emerge solo nella parte in cui si incentra la responsabilità del titolare sulla valutazione dei rischi che i trattamenti comportano rispetto ai diritti e alle libertà, e si commisurano a questa le relative misure di sicurezza da adottare.

Essa emerge anche, e in modo persino più evidente, nelle numerose norme che rimettono agli Stati membri il compito di dettare disposizioni integrative[8]. Centrale è, in questo quadro, il Capo IX, che indica espressamente i settori nei quali spetta agli Stati stabilire, pur nel rispetto dei principi contenuti nel regolamento, le normative relative a settori specifici[9].

Il secondo, e ancor più grave, errore da evitare è pensare che sul piano nazionale ben poco sia destinato a cambiare e che, fermo restando il vincolo al rispetto del regolamento europeo e l'obbligo di adeguare la propria attività ai vincoli imposti dai meccanismi di coerenza e cooperazione, l'Autorità italiana possa, di fatto, continuare a operare nell'ambito del Codice per la protezione dei dati personali italiano vigente.

Una impostazione, questa, che presupporrebbe che per adeguare la normativa italiana e le sue modalità di applicazione al nuovo quadro europeo basti l'attività svolta dall'Autorità, anche attraverso l'adozione di nuove prassi; di Linee Guida rivisitate; di nuovi Codici di comportamento; di nuove modalità per valutare le eventuali perdite di dati denunciate dai titolari o per controllare le analisi di impatto di rischio rispetto alle quali il regolamento prevede il suo intervento.

La realtà è, a mio giudizio, assai più complessa. Merita dunque dedicare qualche rapida riflessione anche all'incidenza che la nuova normativa europea ha rispetto all'ordinamento italiano e alla conseguente necessità di mettere in conto una corposa opera di rivisitazione della normativa contenuta nel Codice attuale, che consenta alla "nuova" Autorità di controllo italiana di operare in modo più efficace e coerente con le innovazioni introdotte.

---

[8] Sul rinvio da parte del regolamento alla legislazione statale "interstiziale" vista, a seconda dei casi, come legislazione di "attuazione", di "armonizzazione", di "completamento", si rinvia a F. Pizzetti, *Privacy e diritto europeo alla protezione dei fatti personali,* vol. II, *Il Regolamento europeo 2016/679,* cit., e *ivi* specialmente paragrafi 4, 5 e 6 della Guida alla lettura.

[9] Cfr. F. Pizzetti, *ibid.*, specialmente paragrafo 7 della Guida alla lettura.

10. Gli effetti del nuovo regolamento sull'ordinamento italiano. Opportunità di un adeguato intervento normativo e rapporti tra le fonti

Per quanto riguarda il ruolo del legislatore statale occorre distinguere i casi in cui il suo intervento è consentito dal regolamento da quelli nei quali esso è indispensabile affinché la nuova normativa possa avere effettiva e completa attuazione nell'ambito dello Stato membro.

Fra i casi in cui l'intervento dello Stato è previsto come possibile, ma non come indispensabile, possono essere citati, ad esempio: l'art. 6, par. 2, che consente agli Stati di introdurre, o mantenere, disposizioni specifiche relativamente alla liceità dei trattamenti per adempiere obblighi legali o compiti di interesse pubblico; l'art. 8, par. 1, che consente agli Stati di fissare un limite inferiore ai sedici anni, ma comunque non sotto i tredici, per la vendita ai minorenni di prodotti della società dell'informazione; l'art. 9, par. 4, che permette agli Stati membri di mantenere, o introdurre, limiti ai trattamenti di dati genetici, biometrici o relativi alla salute, che possono avvenire senza necessità di consenso.

Vi sono poi casi in cui l'intervento dello Stato è previsto come necessario per completare la disciplina regolamentare.

Fra questi è di particolare rilievo tutta la parte del regolamento relativa al nuovo sistema sanzionatorio e alla definizione dei minimi e massimi delle sanzioni da comminare. L'art. 83, infatti, stabilisce solo il limite massimo delle sanzioni comminabili rispetto alle diverse tipologie di violazioni, ma assegna invece agli Stati il compito di definire i limiti minimi. Inoltre, questo stesso articolo rimette agli Stati stabilire in quali casi, e con quali limiti, le sanzioni possano essere estese anche alle autorità pubbliche.

Infine è molto importante, specialmente per l'ordinamento italiano, quanto previsto dall'art. 84, che consente agli Stati membri di stabilire "altre" sanzioni, diverse da quelle stabilite dal regolamento, sia con riferimento alla tipologia sanzionatoria che alla casistica applicabile.

Come è noto, il nostro Codice privacy, nel Titolo III dedicato alla disciplina delle sanzioni, distingue nettamente tra sanzioni amministrative, indicate nel Capo I, e sanzioni penali, indicate nel Capo II. Tenendo conto che il regolamento non prevede mai sanzioni penali, è del tutto ragionevole, e forse persino necessario, che debba essere il legislatore statale a stabilire in modo esplicito se conservare o meno l'apparato sanzionatorio penale, e in quali casi.

Il Considerando 149 consente che gli Stati membri possano stabilire disposizioni relative a sanzioni penali, sia per violazioni del regolamento sia per violazioni di norma nazionali adottate in virtù e nei limiti di questo, specificando inoltre che comunque dovrebbe essere rispettato il principio del *ne bis in idem*. Tuttavia, proprio il fatto che il Considerando specifica che possono essere adottate sanzioni penali nazionali sia rispetto a violazioni di norme regolamentari che di norme statali, ove consentite, impone necessariamente una attenta rivisitazione di un Codice che non distingue affatto, perché adottato sotto la vigenza della direttiva, tra le sanzioni penali per violazioni

regolamentari europee e quelle relative a violazioni di norme nazionali.
Inoltre, nel caso in cui si ritenesse di confermare l'attuale sistema sanzionatorio penale sarebbe assai sconsigliabile contare unicamente sulla rinuncia a ogni modificazione normativa. Immaginare che sia sufficiente una sorta di "silenzio- assenso" per sostenere, senza alcuna esplicita conferma normativa, il perdurare dell'attuale apparato sanzionatorio penale appare assai discutibile in diritto[10], certamente poco condivisibile in fatto.
Occorre inoltre tenere presente che il Codice Privacy italiano fa delle sanzioni penali un uso ampio e rilevante, tanto da costituire da questo punto di vista un *unicum* anche nel panorama europeo. Una ragione ulteriore che invoca la necessità di una rivisitazione esplicita da parte del legislatore di questa parte, sia che la si voglia mantenere sia che, molto più opportunamente, la si voglia sostanzialmente riformare, magari rinunciando al ricorso stesso alla sanzione penale, sia per violazioni a norme regolamentari che nazionali, se non in casi di assoluta pericolosità e allarme sociale.
A questo va aggiunto che, come esplicitamente prevedono sia l'art. 83, par. 9, sia l'art. 84, ogni sanzione pecuniaria o penale che gli Stati adottino oltre a quelle previste dal regolamento, devono essere comunicate alla Commissione entro il 25 maggio 2018.
Una ragione in più per ritenere poco sostenibile mantenere intatto l'attuale apparato sanzionatorio senza che il legislatore assuma alcuna iniziativa, e senza che l'Autorità provveda a darne comunicazione alla Commissione.
Lo stesso ragionamento, sempre sul versante del sistema sanzionatorio, va fatto tenendo conto che il Considerando 150 prevede che gli Stati membri possano, in certi casi, individuare anche soltanto nel semplice "avvertimento" la sanzione da applicare[11].
Si tratta di un'ipotesi che il nostro Codice non conosce, cosicché sarebbe quanto meno audace pensare di affidare all'Autorità e alle sue prassi il potere di applicare questa sanzione anche in assenza di ogni innovazione normativa.
Tra le norme del regolamento che consentono agli Stati l'adozione di discipline derogatorie sono molto importanti anche quella in materia di profilazione e trattamenti automatizzati, di cui all'art. 22 e quella, contenuta nell'art. 23, che consente agli Stati di limitare la responsabilità dei titolari e dei responsabili dei trattamenti con riguardo

[10] Un tema ancora tutto da affrontare è infatti il rapporto che sussisterà dopo il 25 maggio 2018 tra la fonte regolamentare comunitaria in materia di protezione dei dati personali e la fonte statale che disciplina nella stessa materia. La questione si porrà sotto almeno due profili diversi ma egualmente importanti. Da un lato si dovrà risolvere l'eventuale contrasto diretto tra norma regolamentare e norma statale nelle materie in cui non è consentita una legislazione statale derogatoria. In questi casi si dovrà affermare, senza ombra di dubbio, la prevalenza della norma europea. Dall'altro si dovrà sciogliere il nodo del rapporto tra norma regolamentare che consente deroghe alla legislazione statale e leggi statali precedenti l'entrata in vigore del regolamento o comunque la sua piena attuazione. Non vi è dubbio che se la legge statale è successiva all'entrata in vigore della norma regolamentare o alla sua attuazione e dispone nell'ambito delle materie derogabili, allora prevarrà la normativa statale. Meno certo invece se si potrà sostenere la stessa cosa nel caso in cui la normativa statale, pur relativa alle materie derogabili, sia antecedente all'entrata in vigore del Regolamenti o addirittura alla sua stessa approvazione.

[11] Invero nel Considerando 150 non è chiarissimo se l'avvertimento è considerato una sanzione o cosa diversa dalla sanzione come tale. In ogni caso resta fermo che il Codice italiano non conosce questo tipo di provvedimento correlato all'accertamento di una violazione e dunque occorrerebbe certamente operare almeno secondo quanto indicato nel testo.

agli obblighi e ai diritti del Capo III, sempre che ricorrano le cause legittimanti e siano rispettati i contenuti minimi previsti dal medesimo articolo.

11. La riserva alla legislazione degli Stati della disciplina in settori specifici

Ai casi finora richiamati si devono poi aggiungere quelli in cui il regolamento riserva agli Stati la regolazione di particolari settori.

Meritano di essere richiamati i casi contenuti nel Capo IX, che riguardano specificamente i trattamenti relativi alla libertà di espressione e di informazione (art. 85); il trattamento e accesso del pubblico ai documenti ufficiali (art. 86); il trattamento del numero identificativo nazionale (art. 87); i trattamenti nell'ambito dei rapporti di lavoro (art. 88); le garanzie e deroghe per trattamenti di archiviazione e di ricerca scientifica, storica o statistica (art. 89); gli obblighi di segretezza (art. 90).

Agli Stati membri spetta anche la competenza in materia di norme relative ai trattamenti nell'ambito delle chiese o associazioni religiose (art. 91).

Sono tutti settori nei quali la legislazione specifica è riservata agli Stati in virtù delle peculiarità, anche culturali e religiose, che possono caratterizzare i diversi ordinamenti. Questo peraltro non esclude che gli Stati incontrino anche limiti specifici stabiliti dal regolamento stesso, oltre alla necessità di rispettare i principi comuni. Quello che è certo, però, è che spetta al legislatore statale esercitare il potere normativo, avendo cura di rispettare vincoli e principi posti in via generale dal regolamento, che costituiscono limite anche al potere "esclusivo"[12] degli Stati.

Va inoltre sottolineato che nelle materie rimesse alla regolazione nazionale è fatto obbligo agli Stati di dare tempestiva comunicazione alla Commissione delle norme adottate. Questo vale particolarmente per la disciplina statale in materia di libertà di espressione e informazione, di trattamento dati nell'ambito dei rapporti di lavoro, di deroghe ai trattamenti dati a fini di archiviazione, di ricerca scientifica o storica e di ricerca statistica.

Dunque, anche rispetto a questi settori è da chiedersi se eventuali deroghe alle disposizioni regolamentari contenute nel Codice Privacy italiano e le disposizioni nazionali vigenti nei settori di competenza statale debbano essere almeno oggetto di conferma legislativa, o comunque di comunicazione alla Commissione entro il 25 maggio 2018, e quale debba essere il ruolo della Autorità rispetto a tali comunicazioni.

[12] È ovvio che la dizione potere "esclusivo" degli Stati è una formula mutuata dall'esperienza costituzionale italiana, che però riguarda il potere esclusivo dello Stato nell'ambito della ripartizione delle competenze legislative tra Stato e regioni. L'analogia è volutamente un poco forzata ma può esser utile, anche tenendo conto che, come si dice un po' sinteticamente nel testo, il legislatore statale nelle materie del Capo IX incontra sia il limite della competenza, che è limitata alle materie indicate, sia i limiti costituiti dai principi e vincoli generali del regolamento. Limiti, questi, che ovviamente incontra anche il legislatore statale nelle materie di sua competenza esclusiva *ex* art. 117, c. 2, Cost., in quanto anche in queste materie esso è vincolato dalla Costituzione.

12. Gli obblighi statali di attuazione del regolamento

Da ultimo, merita richiamare le norme regolamentari che pongono in capo agli Stati veri e propri obblighi di attuazione.
Fra queste le più importanti, e anche le più urgenti da adottare, sono quelle contenute nel Capo VI che riguardano direttamente le Autorità di controllo.
Anche se la legislazione italiana vigente appare in questo ambito già ampiamente conforme al nuovo regolamento, è ovvio che non è pensabile che le poche e scarne norme previste nel Titolo II della Parte terza dell'attuale Codice italiano in materia di protezione dei dati personali[13] bastino a soddisfare tutti gli obblighi che il regolamento pone a carico degli Stati.
Del resto sarebbe ben strano che un apparato normativo rielaborato nel 2003 sotto l'impero della direttiva e, per questa parte, sostanzialmente immodificato, non richiedesse alcun adeguamento a un quadro normativo che vede profondamente mutato il ruolo delle Autorità di controllo, i rapporti che intercorrono tra di loro nell'ambito dei meccanismi di coerenza e un sostanziale ridisegno del ruolo, compiti e poteri del Gruppo di lavoro comune.
È evidente che, anche nell'ipotesi che la normativa nazionale sia, come quella italiana, adeguata anche al nuovo regolamento per quanto attiene all'indipendenza assicurata all'Autorità e alle procedure di nomina (e forse anche ai requisiti dei membri che la compongono), sarà inevitabile che il legislatore, ovviamente sentita l'Autorità stessa, provveda ad adeguare le risorse finanziarie, umane e strumentali al forte incremento di compiti, poteri e attività che il regolamento prevede. Nel contempo, potrebbe essere utile anche cogliere l'occasione per definire meglio requisiti e procedure di nomina dei membri, prevedendo anche procedure di selezione e verifica dei requisiti più trasparenti, ferma restando l'elezione da parte del Parlamento.
In questo quadro potrebbe essere utile anche una normativa più adeguata dell'attuale per quanto riguarda i rapporti tra l'Autorità di controllo in materia di protezione dei dati personali e le altre Autorità di regolazione, sia per segnare meglio i confini tra i diversi ambiti di competenza, specialmente nel settore delle telecomunicazioni e della società digitale, sia per definire in modo più strutturato le eventuali forme di raccordo e cooperazione. Sembra ragionevole ritenere, infatti, che sempre più in futuro anche le Autorità indipendenti di regolazione e di controllo debbano essere chiamate a interagire fra loro, specialmente se si condivide la tesi che col nuovo regolamento anche la protezione dei dati personali non abbia più un orizzonte limitato soltanto alla tutela del diritto fondamentale dell'interessato.
In ogni caso il rinvio alla legislazione statale di ambiti di decisione molto ampi in materia di indipendenza, organizzazione, composizione, esercizio delle competenze e dei poteri delle Autorità, indica che, almeno rispetto all'ordinamento italiano, è certamente necessario un ampio e incisivo intervento legislativo.
Intervento che, come quelli relativi alle norme interstiziali e integrative precedente-

[13] Ovviamente il riferimento è al decreto legislativo 30 giugno 2003 n. 196 e successive modificazioni, generalmente indicato più brevemente come Codice privacy)

mente citate, deve avvenire, per esplicita previsione normativa, entro il 25 maggio 2018. L'art. 51, par. 1, è infatti molto esplicito su questo punto: «Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del presente Capo al più tardi entro maggio 2018, e comunica senza ritardo ogni successiva modifica».

Si tratta dunque di un impegno che il legislatore italiano è chiamato ad assolvere entro un termine molto breve e rigorosamente fissato.

Il primo e fondamentale compito che il legislatore statale deve assolvere, e in modo anche tempestivo considerando i pochi mesi a disposizione, è quello di adempiere a quanto previsto dall'art. 52, par. 4.

Si tratta della norma regolamentare che, anche a rafforzamento e garanzia dell'indipendenza che deve essere assicurata all'Autorità di controllo, stabilisce: «ogni Stato membro provvede affinché ogni Autorità di controllo sia dotata delle risorse umane, tecniche e finanziarie, dei locali e delle infrastrutture necessari per l'effettivo adempimento dei suoi compiti e l'esercizio dei propri poteri, compresi quelli nell'ambito dell'assistenza reciproca, della cooperazione e della partecipazione al Comitato».

Si tratta di una disposizione che va oltre il quadro strettamente nazionale, anche se è al legislatore nazionale che si rivolge.

Non va mai dimenticato, infatti, che nel regolamento le Autorità di controllo hanno un forte dovere di collaborazione tra loro, sia nell'ambito delle attività di cooperazione e coerenza disciplinate nel Capo VII, sia per quanto riguarda i rapporti tra di loro e nei confronti dell'eventuale *leading authority*, sia infine nell'ambito del Comitato europeo per la protezione dei dati, disciplinato nel Capo VIII.

La legislazione chiamata ad attuare quanto previsto dall'art. 52 ha necessariamente un rilievo che va oltre le stesse frontiere nazionali, e presenta un interesse specifico per tutto il sistema di protezione dei dati personali dell'Unione. Si tratta di un aspetto molto importante, che forma oggetto anche di una specifica previsione regolamentare contenuta nell'art. 51, par. 2, che precisa «Ogni Autorità di controllo contribuisce alla coerente applicazione del presente regolamento in tutta l'Unione. A tale scopo, le autorità di controllo cooperano tra loro e con la Commissione, conformemente al Capo VII».

Siamo dunque in presenza di un obbligo che incombe su ogni Stato membro e il cui adempimento ha un esplicito valore non solo nell'ambito del rispetto formale del regolamento ma anche, e soprattutto, nel quadro della cooperazione tra gli Stati membri all'interno dell'Unione.

Tutto questo spiega anche perché il già citato art. 51, par. 4, imponga esplicitamente e tassativamente ad ogni Stato membro di comunicare alla Commissione le disposizioni di legge relative alla disciplina della propria Autorità nazionale di controllo, in modo che la Commissione ne possa tempestivamente verificare la conformità a quanto previsto dal regolamento.

Si tratta di un nodo cruciale, che è bene sia molto chiaro a tutti.

Anche chi, forse un po' affrettatamente, ritenesse che la normativa italiana già in vigore non abbia bisogno di interventi normativi di adeguamento al regolamento, deve mettere in conto che in ogni caso di questo va data comunicazione alla Commissione

entro il 25 maggio 2018.
Si deve inoltre tenere presente che tale scelta, certamente non facile da sostenere, sarebbe comunque sottoposta al vaglio della Commissione, con esito almeno problematico, specialmente per quanto riguarda la conformità della regolazione interna dell'Autorità ai compiti che essa deve assolvere nel quadro dei meccanismi di cooperazione previsti dal regolamento, e in particolare di quanto indicato nel Capo VII.
Se invece ci si orienta a ritenere, come sembra necessario, che occorrano comunque corposi interventi legislativi per adeguare anche la attuale normativa relativa all'Autorità italiana al nuovo quadro europeo, è importante che l'Autorità stessa segnali con forza al Governo e al Parlamento la necessità di provvedere, indicando anche le soluzioni che ritiene preferibili e le lacune della attuale legislazione che è indispensabile colmare.

13. La protezione dei dati personali e le Autorità garanti come presidio di libertà nella società digitale.

Siamo così giunti al termine delle considerazioni che la lettura della raccolta di scritti contenuta nel volume, e il nuovo quadro regolatorio europeo ormai in vigore, hanno stimolato e suggerito.
Del valore che il volume ha si è già detto, e di ciò deve essere dato atto all'iniziativa lodevolissima dei curatori e ai contributi degli autori.
La riflessione qui sviluppata va però ben oltre.
Il tentativo, forse troppo audace, che si è cercato di fare è quello di guardare avanti e di indicare almeno gli aspetti del nuovo regolamento che più sfidano sia il legislatore nazionale che l'Autorità garante, senza peraltro dimenticare di sottolineare anche le molte e fondamentali innovazioni che il nuovo quadro regolatorio introduce nel diritto europeo alla protezione dei dati personali.
Quello che è certo è che ormai è iniziata una nuova stagione, nella quale la tutela del diritto fondamentale alla protezione dei dati dei cittadini europei si amplia enormemente.
Questo avviene su due piani: il primo è quello della tutela dei dati personali, che non è più solo difesa del diritto dei singoli ma garanzia per tutta la società europea; il secondo è quello di una normativa solidamente definita ma anche molto flessibile, capace di regolare in modo adeguato anche i futuri, ma già oggi prevedibili, sviluppi della società digitale.
A questi due aspetti se ne aggiunge un terzo: il ruolo delle Autorità di controllo, sia viste nella loro dimensione nazionale che nella loro attività di cooperazione a livello di Unione.
Proprio il rinnovato e rafforzato ruolo delle Autorità è l'elemento di maggiore interesse, specialmente nel momento in cui, con il volume, si vuole celebrare il primo ventennio di attività dell'Autorità italiana.
Le Autorità sono destinate a svolgere un ruolo sempre più centrale per la tutela delle libertà dei cittadini europei, persino oltre la difesa dei loro dati personali. Esse sono infatti le istituzioni che hanno la maggiore competenza e la più ampia esperienza in

materia di dati e dei loro trattamenti rispetto ad ogni altra Istituzione europea.
Viviamo in un mondo nel quale sempre più la dimensione della realtà digitale e quella della realtà reale si intrecciano fra loro mentre la prospettiva di una civiltà dominata dai Big Data[14], dalla Intelligenza Artificiale, dall'Internet delle cose[15], è già nel nostro presente e ancor più nel nostro prossimo futuro. In questo quadro è evidente che, senza una adeguata regolazione dei trattamenti dei dati e una costante attività di vigilanza e di controllo su come questi sono utilizzati, conservati, protetti, sono le nostre stesse libertà ad essere a rischio.
Mai come oggi è evidente che nessuno più delle Autorità di protezione dei dati personali è in prima fila nello sforzo di tutelare e difendere i diritti di libertà dei moderni nell'ambito di una società che promette un presente/futuro ricco di opportunità ma anche carico di rischi.
Alle Autorità è affidato dunque molto del futuro della civiltà europea e dei diritti che essa ha faticosamente costruito in secoli di lotte e di storia.
L'augurio che come italiani ed europei facciamo al Garante nel suo ventesimo anno di vita è che esso, nei tempi complicati che ci attendono, possa essere sempre più all'altezza del suo passato e, soprattutto, del suo futuro.

[14] A conferma che più il mondo digitale è complesso più è necessario una forte tutela dei dati e, in particolare, dei dati personali, è importante sottolineare lo sforzo compiuto dal Comitato consultivo della Convenzione 108 della CEDU che ha affrontato per primo il tema della sfida posta dai Big Data in questo ambito. Cfr. *Consultative Committe of the Convention for the protection of individuals with regard to automatic processing of personal data*, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, Strasbourg, 23 January, 2017. Sul rapporto tra protezione dei dati personali e Big Data cfr. però anche Gruppo di lavoro Articolo 29, *Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*, Bruxelles, 16 September 2014, WP221

[15] Sul tema dell'Internet delle cose le Autorità europee di protezione dati si sono già occupati anche sotto l'impero della direttiva, ma mentre era già in discussione l'esame del progetto di nuovo regolamento. Cfr. Gruppo di lavoro Articolo 29, *Opinion 8/2014 on the Recent Developments on the Internet of Things*, Bruxelles, 16 September 2014,WP223