GIUSELLA FINOCCHIARO (*)
Professore nell'Università di Bologna

INTRODUZIONE AL REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI

SOMMARIO: 1. Il percorso storico. – 2. Il diritto alla protezione dei dati personali e il diritto alla riservatezza. – 3. Le esigenze alla base del reg. UE 2016/679. – 4. Il reg. UE 2016/679 in sintesi. – 5.1. Le novità più rilevanti. Il nuovo approccio al rischio. Il principio di *accountability*. – 5.2. Il criterio di ragionevolezza. – 5.3. Ambito di applicazione territoriale. – 5.4. Il necessario bilanciamento di interessi.

1. *Il percorso storico.*

Il nuovo regolamento europeo sulla protezione dei dati personali (1) aggiunge una nuova tappa ad un percorso iniziato almeno venti anni fa. È del 1996, infatti, la cosiddetta "Direttiva madre" in materia di trattamento dei dati personali, la dir. 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Essa aveva recepito un dibattito culturale e un pensiero dottrinale sviluppatosi nei decenni precedenti e delineato un modello statico di trattamento dei dati personali, ormai superato. Diversa all'epoca anche la tecnologia: era un mondo privo di *smart phone*, *social network* e motori di ricerca. Il modello normativo individuava un unico scambio di dati: dall'interessato al titolare del trattamento. La realtà dei *social network* e dei motori di ricerca, di un modo digitalmente sempre interconnesso,

(*) Contributo pubblicato previo parere favorevole espresso da un componente del *Comitato per la valutazione scientifica*.

(1) Per un approfondimento in merito alla nuova normativa in materia di protezione dei dati personali si rinvia a PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, 2016 e RESTA-ZENO ZENCOVICH, *La protezione transnazionale dei dati personali dai* "safe harbour principles" *al* "privacy shield", Roma, 2016.

invece, si basa su un modello di condivisione e di cogestione di dati e informazioni, destinati fin dall'origine ad una circolazione globale.

Nell'ordinamento giuridico italiano, come è noto, il diritto alla protezione dei dati personali è stato introdotto con la l. 31 dicembre 1996, n. 675, "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" ed è stato sancito dall'art. 1 del d.lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, che recita: "chiunque ha diritto alla protezione dei dati personali che lo riguardano" (2).

Dunque da almeno venti anni il diritto alla protezione dei dati personali è positivamente riconosciuto e distinto dal diritto alla riservatezza.

2. *Il diritto alla protezione dei dati personali e il diritto alla riservatezza.*

Il diritto alla protezione dei dati personali consiste nel diritto del soggetto cui i dati si riferiscono, di esercitare un controllo, anche attivo, su detti dati, diritto che si estende dall'accesso alla rettifica (3).

Il diritto alla protezione dei dati personali è riconosciuto dalla Carta dei diritti fondamentali dell'Unione europea la quale, nell'affermare tale diritto, ribadisce alcuni principi contenuti nella dir. 95/46/CE (4). All'art. 8 della Carta, infatti, significativamente fra i diritti di libertà, si afferma il

---

(2) Per un inquadramento della evoluzione del diritto alla *privacy* che ha portato alla elaborazione di un distinto diritto alla protezione dei dati personali, si v. BUSNELLI, *Nota introduttiva al commento della l. 31 dicembre 1996, n. 675. Spunti per un inquadramento sistematico*, in AA.VV., *Tutela della privacy*, BIANCA, BUSNELLI, BELLELLI, LUISO, NAVARETTA, PATTI e VECCHI (Commentario a cura di), Padova, 1999, p. 228 e ss.

(3) Ho approfondito il tema nel mio *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, p. 1 ss.

(4) La Carta dei diritti fondamentali dell'Unione europea proclamata il 7 dicembre 2000 è stata pubblicata in *G.U.C.E.* 2000/C-364/01. Al riguardo, cfr. Autorità Garante per la protezione dei dati personali, Relazione 2000, Roma, Presidenza del Consiglio dei Ministri, 2001, p. 262. In dottrina, RESCIGNO, *La Carta dei diritti fondamentali dell'Unione europea*, Torino, 2003; sul successivo progetto di Trattato istitutivo la Costituzione europea, MANZELLA, MELOGRANI, PACIOTTI RODOTÀ, *Riscrivere i diritti in Europa. Introduzione alla Carta dei diritti fondamentali dell'Unione europea*, Bologna, 2001 e BARBERA, *La Carta europea dei diritti e la Costituzione italiana*, in *Le libertà e i diritti nella prospettiva europea*, Padova, 2002, p. 107.

Relativamente alla dir. 1995/46/CE, utile il riferimento ai *considerando*, dai quali si evince la consapevolezza per cui dall'integrazione economica e sociale, successiva alla instaurazione e al funzionamento del mercato interno, deriva un sensibile aumento dei flussi transnazionali di dati personali cui deve corrispondere, necessariamente, un livello di tutela dei diritti e delle libertà delle persone relativamente al trattamento dei dati personali equivalente in tutti gli Stati membri. Per un'analisi generale della dir. 95/46/CE, si v. MACARIO, *La protezione dei dati personali nel diritto privato europeo*, in CUFFARO e RICCIUTO (a cura di), *La disciplina del trattamento di dati personali*, Torino, 1997.

diritto alla protezione dei dati personali, e precisamente che ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Si afferma, inoltre, che i dati personali devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o ad un altro fondamento legittimo previsto dalla legge e che ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Sempre nell'art. 8 si afferma che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Tale diritto è distinto dal diritto alla protezione della vita privata, altra formulazione del diritto alla riservatezza, riconosciuto dall'art. 7 della Carta, ove si afferma il diritto al rispetto della vita privata e della vita familiare: ogni individuo, dispone la norma, ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni.

Il diritto alla protezione dei dati personali ha un oggetto estremamente vasto, che è conseguenza della stessa definizione di dato personale.

Infatti, l'ambito individuato dalla definizione di dato personale è amplissimo: costituisce dato personale "qualsiasi informazione riguardante una persona fisica identificata o identificabile ('interessato'); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *on line* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale" (5). Il dato personale è, quindi, qualunque informazione riferibile a qualunque soggetto, anche se costituita da suoni o immagini. Sono, invece, esclusi dall'ambito di applicazione della normativa i dati anonimi. è definito dato anonimo dalla legge italiana "il dato che in origine, o a seguito di trattamento, non può essere associato a un interessato identificato o identificabile" (6).

Muovendo, dunque, dall'ampia definizione di dato personale, il diritto alla protezione dei dati personali si configura come il diritto di un soggetto di controllare l'insieme delle informazioni che a questi si riferiscono e che quindi costituiscono il suo riflesso e delineano lo stesso suo essere nella società dell'informazione (7).

---

(5) Il dato personale viene così definito dall'art. 4, n. 1, reg. UE 2016/679.

(6) Sull'anonimato si rinvia a FINOCCHIARO (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, in *Trattato di diritto commerciale e diritto pubblico dell'economia*, GALGANO (diretto da), vol. XLVIII, Padova, 2008, con ampia bibliografia.

(7) Così RODOTÀ, allora Presidente dell'Autorità Garante per la protezione dei dati personali, sulla nozione di "corpo elettronico", nella Relazione 2002 sull'attività dell'Auto-

Il diritto alla protezione dei dati personali è anche noto come "*information privacy*", "*informational privacy*", "*data privacy*", tutte espressioni nelle quali si evidenzia che l'oggetto del diritto è l'informazione o il dato, benché a rigore dato e informazione siano termini non coincidenti (8).

Il diritto alla protezione dei dati personali deve essere considerato distinto dalla libertà negativa di non subire interferenze nella propria vita privata, al cuore del diritto alla riservatezza, costituendo invece il fondamento della libertà positiva di esercitare un controllo sul flusso delle proprie informazioni. Per questa ragione è frequente che il diritto alla protezione dei dati personali sia inteso come diritto all'autodeterminazione informativa, cioè alla scelta di ogni soggetto di autodefinirsi e determinarsi (9).

Il diritto alla riservatezza è, come è noto, il diritto di creazione giurisprudenziale consistente nell'escludere altri dalla conoscenza di vicende strettamente personali e familiari. A differenza del diritto alla protezione dei dati personali è un diritto a contenuto negativo, quello di non fare conoscere e di mantenere riservate alcune informazioni, piuttosto che a contenuto positivo, quello cioè di esercitare un controllo sulle medesime. Inoltre, a differenza del diritto alla protezione dei dati personali, non ha ad oggetto le informazioni, di qualunque natura esse siano, ma soltanto le vicende riservate.

Il diritto alla riservatezza viene generalmente ricondotto al famoso articolo di Warren e Brandeis sul '*right to be let alone*' (10) inteso come riconoscimento della inviolabilità della sfera personale e della propria vita privata. Ma da autorevole parte della dottrina viene ricondotto alla dottrina tedesca (11).

---

rità Garante per la protezione dei dati personali, Roma, Presidenza del Consiglio dei Ministri, 20 maggio 2003; ID., *Tecnologie e diritti*, Bologna, 1995.

(8) Su questo punto si avrà modo di soffermarsi più avanti.

(9) Sulla relazione fra diritto alla protezione dei dati personale e diritto all'identità personale v. BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997, p. 103 e ss.

(10) WARREN-BRANDEIS, *The right to privacy*, 15 dicembre 1890, 4 Harvard Law Review, 193-220, ripubblicato dall'Autorità Garante per la protezione dei dati personali.

(11) Cfr. per tutti BUSNELLI, *Nota introduttiva al commento della l. 31 dicembre 1996, n. 675. Spunti per un inquadramento sistematico*, in AA.VV., *Tutela della privacy*, BIANCA, BUSNELLI, BELLELLI, LUISO, NAVARETTA, PATTI VECCHI (Commentario a cura di), cit., p. 228 e ss. Per un inquadramento sistematico del diritto alla riservatezza si rinvia ad AULETTA, *Riservatezza e tutela della personalità*, Milano, 1978 e RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 209 e ss.

In Italia, il diritto alla riservatezza è stato riconosciuto dalla Corte di Cassazione nel 1975 (12), mentre la stessa Corte con la sentenza n. 4487 del 1956 aveva negato tale diritto.

Con la pronuncia del 1975, la Corte individua il fondamento del diritto alla riservatezza nelle norme ordinarie e costituzionali che tutelano aspetti peculiari della persona, nonché nelle disposizioni, rinvenibili in leggi speciali, che richiamano espressamente la vita privata della persona (13).

Il diritto alla riservatezza è riconosciuto a livello internazionale (14) dalla Convenzione di Strasburgo (15) e dall'art. 7 della Carta dei diritti fondamentali dell'Unione europea.

Il diritto alla protezione dei dati personali e il diritto alla riservatezza hanno ambiti molto diversi e soprattutto hanno oggetti diversi. Naturalmente ci sono dei casi in cui i due diritti coincidono. Ad esempio un dato sanitario contenuto nella cartella clinica di un paziente è oggetto sia del diritto alla riservatezza che del diritto alla protezione dei dati personali. Ma ci sono casi in cui questi diritti non coincidono e le informazioni sono tutelate solo dal diritto alla protezione dei dati personali.

3. *Le esigenze alla base del reg. UE 2016/679.*

Il Regolamento europeo sulla protezione dei dati personali nasce, come ampiamente illustrato nei considerando (16), dalla constatazione della frammentazione della disciplina sulla protezione dei dati personali nell'U-

---

(13) Si legge nella motivazione della sentenza: "il nostro ordinamento riconosce il diritto alla riservatezza che consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non sono giustificati da interessi pubblici preminenti". Successivamente, con la sentenza del 9 giugno 1998 n. 5658, la Corte di Cassazione ha sottolineato che le vicende oggetto della riservatezza si riferiscono ad una "certa sfera della vita individuale e familiare, all'illesa intimità personale in certe manifestazioni della vita di relazione, a tutte quelle vicende cioè, il cui carattere intimo è dato dal fatto che esse si svolgono in un domicilio ideale, non materialmente legato alle mura domestiche".

(14) A livello universale, l'art. 12 della Dichiarazione universale dei diritti dell'uomo, ripreso in termini quasi identici dall'art. 17 del Patto sui diritti civili e politici del 1966, sancisce che "nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesioni del suo onore e della sua reputazione".

(15) Convenzione del Consiglio d'Europa n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, Strasburgo, 28 gennaio 1981.

(16) Così 9° considerando.

nione europea e dalla rilevazione della diffusa incertezza giuridica concernente l'applicazione della normativa.

L'esigenza è quella di assicurare un'applicazione omogenea della normativa vigente, al fine di creare un clima di fiducia per lo sviluppo economico negli ambienti *on line*. Un quadro giuridico incerto costituisce, infatti, un freno allo sviluppo dell'economia digitale. Anche da queste considerazioni deriva la scelta dello strumento giuridico utilizzato: regolamento e non direttiva.

Conseguentemente, trattandosi di regolamento, esso sarà direttamente applicabile in tutti gli Stati membri dell'Unione europea, senza la necessità di atti di recepimento nei singoli Stati nazionali.

Non si tratta più di uno strumento di armonizzazione, ma invece di uno strumento di uniformazione del diritto per gli Stati europei, eliminando così in radice quelle piccole differenze che rendono difficile realizzare compiutamente un mercato unico.

Come con molti altri atti normativi europei in questo settore, con esso si intende rafforzare la fiducia nelle transazioni elettroniche nel mercato interno, assicurando la protezione dei dati personali, e aumentando così l'efficacia dei servizi *on line* pubblici e privati nell'Unione europea.

Peraltro, in questo quadro, non si può non considerare il reg. UE n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014, "in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE" (17).

I due regolamenti, considerati in una prospettiva unitaria, indicano chiaramente l'intento del legislatore europeo di disegnare un mercato unico digitale, rimuovendo gli ostacoli giuridici costituiti dalla disomogeneità delle norme applicabili.

Oltre a ciò, emerge, inoltre, la volontà del legislatore europeo di consolidare la posizione europea nel quadro globale, affermando un approccio unitario, che declina i principi fondamentali statuiti dalla Carta dei diritti fondamentali dell'Unione europea.

---

(17) Pubblicato in *G.U.U.E.* L 257 del 28 agosto 2014.

Il Regolamento è, in sigla, comunemente denominato "eIDAS", dove "e" sta per "*electronic*", "ID" per "*identification*", "A" per "*authentication*" e "S" per "*signature*".

Per un commento si rinvia al mio *Una prima lettura del regolamento europeo eIDAS: identificazione* on line, *firme elettroniche e servizi fiduciari*, in questa *Rivista*, 2015, p. 419 ss.

4. *Il reg. UE 2016/679 in sintesi.*

Il reg. UE 2016/679 raccoglie l'esperienza maturata in Europa negli ultimi venti anni e dunque, quasi fosse un testo unico, cerca di riordinare e razionalizzare [18]. In questo senso vanno lette alcune disposizioni, che non hanno un contenuto innovativo con riguardo all'esperienza italiana, ma che certamente arricchiscono il testo della previgente normativa europea. Fra queste, ad esempio, quelle concernenti il consenso [19].

Alcune definizioni sono invece nuove, come quella di dati biometrici [20] e quella di pseudonimizzazione [21].

In altre, sono state aggiunte delle precisazioni, come con riferimento all'informativa [22].

---

[18] Il 3 gennaio 2017, il Gruppo di lavoro articolo 29 per la protezione dei dati ha adottato il suo secondo piano d'azione per l'implementazione del Regolamento entro il 2018, aggiornando il precedente piano d'azione adottato il 2 febbraio 2016. In particolare, con il nuovo *action plan* il Gruppo di lavoro articolo 29 per la protezione dei dati si impegna ad ultimare le attività intraprese nel 2016 (tra cui l'adozione di linee guida sulla valutazione d'impatto e la predisposizione del meccanismo di coerenza e del *one-stop-shop*) e prevede l'adozione di nuove misure per agevolare l'uniforme applicazione del Regolamento (per esempio attraverso l'emanazione di linee guida sul consenso e sulla profilazione).

[19] Si precisa, infatti, che nel Regolamento il consenso, inteso come qualsiasi manifestazione di assenso dell'interessato, deve essere libero, specifico, informato e inequivocabile, cioè espresso mediante dichiarazione o azione positiva inequivocabile. Rispetto all'attuale disciplina è invece innovativa la previsione introdotta dall'art. 7 in cui si precisa che "qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali". Con tale disposizione sembra, infatti, che il Regolamento ponga in capo al titolare un vero e proprio onere della prova sulla raccolta del consenso.

[20] Il Regolamento definisce dati biometrici "i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici".

[21] La pseudonimizzazione è definita dal Regolamento come "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

[22] La nuova normativa, infatti, da un lato prevede espressamente un generale dovere di trasparenza in capo al titolare, disponendo che tutte le informazioni fornite all'interessato devono essere comunicate "in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente a minori". Dall'altro lato, introduce ulteriori informazioni tra quelle che il titolare deve comunicare all'interessato ai sensi dell'art. 13, prima assenti nel testo sia della dir. 1995/46/CE sia del Codice italiano (in particolare, viene inserito il dovere di comunicare l'intenzione del titolare di trasferire dati personali a un paese terzo e la base giuridica di

Ancora, è stato inserito un articolo *ad hoc* sul consenso dei minori (23).

Sono stati dettagliatamente disciplinati alcuni diritti, quali il diritto alla cancellazione dei dati, già noto come "diritto all'oblio" (24), con un impatto di gran lunga minore rispetto a quello annunciato, limitandosi la novità alla previsione che il titolare deve informare i terzi della richiesta dell'interessato di cancellare i *link* ai suoi dati, copie e riproduzioni (25).

È stato introdotto il diritto alla portabilità dei dati (26), cioè il diritto di trasferire i propri dati da un sistema di trattamento elettronico ad un altro.

In parte nuova e certamente di grande rilevanza la disciplina sul trasferimento dei dati all'estero: essa è più articolata e meglio strutturata e si prevede espressamente il ruolo dell'autorità di controllo capofila e la disciplina dello sportello unico (27).

---

tale trasferimento, il periodo di conservazione dei dati personali o i criteri utilizzati per determinare tale periodo e l'esistenza di un processo decisionale automatizzato).

(23) L'art. 8, comma 1° prevede che qualora l'interessato abbia espresso il suo consenso "per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tal trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale".

(24) Ho approfondito il tema del diritto all'oblio nei miei *La memoria della rete e il diritto all'oblio*, in *Dir. inf.*, 2010, 391 e *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Dir. inf.*, 2014, 591-604, pubblicato inoltre in AA.VV., *Internet e Diritto civile*, PERLINGIERI e RUGGERI (a cura di), Napoli, 2015.

(25) In particolare, l'art. 17, comma 2° prevede che il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato a cancellarli, "tenendo conto della tecnologia disponibile e dei costi di attuazione adotta misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali".

(26) Il diritto alla portabilità è, ai sensi dell'art. 20, comma 1°, il diritto dell'interessato "di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora: a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e b) il trattamento sia effettuato con mezzi automatizzati".

Sul tema si è espresso anche il Gruppo di lavoro articolo 29 per la protezione dei dati con l'adozione delle "*Guidelines on the right to data portability*" del 13 dicembre 2016.

(27) Con riferimento alle competenze dell'autorità capofila, l'art. 56 recita: "Fatto salvo l'articolo 55, l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare e del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento, secondo la procedura di cui all'articolo 60.

2. In deroga al paragrafo 1, ogni autorità di controllo è competente per la gestione dei reclami a essa proposti o di eventuali violazioni del presente regolamento se l'oggetto riguarda unicamente uno stabilimento nel suo Stato membro o incide in modo sostanziale

Sono previsti alcuni meccanismi per garantire un'applicazione uniforme del Regolamento nell'Unione europea, attraverso il c.d. "meccanismo di coerenza" ([28]).

Mutano le disposizioni sul foro competente, con le previsioni di più fori alternativi ([29]), nonché il regime di responsabilità civile, che pare non individuare più un regime di responsabilità oggettiva ([30]) come attualmente previsto dalla normativa italiana vigente.

---

sugli interessati unicamente nel suo Stato membro.

3. Nei casi indicati al paragrafo 2 del presente articolo, l'autorità di controllo informa senza indugio l'autorità di controllo capofila in merito alla questione. Entro un termine di tre settimane da quando è stata informata, l'autorità di controllo capofila decide se intende o meno trattare il caso secondo la procedura di cui all'articolo 60, tenendo conto dell'esistenza o meno di uno stabilimento del titolare del trattamento o responsabile del trattamento nello Stato membro dell'autorità di controllo che l'ha informata.

4. Qualora l'autorità di controllo capofila decida di trattare il caso, si applica la procedura di cui all'articolo 60. L'autorità di controllo che ha informato l'autorità di controllo capofila può presentare a quest'ultima un progetto di decisione. L'autorità di controllo capofila tiene nella massima considerazione tale progetto nella predisposizione del progetto di decisione di cui all'articolo 60, paragrafo 3.

5. Nel caso in cui l'autorità di controllo capofila decida di non trattarlo, l'autorità di controllo che ha informato l'autorità di controllo capofila tratta il caso conformemente agli articoli 61 e 62.

6. L'autorità di controllo capofila è l'unico interlocutore del titolare del trattamento o del responsabile del trattamento in merito al trattamento transfrontaliero effettuato da tale titolare del trattamento o responsabile del trattamento".

Sull'individuazione dell'autorità capofila (*lead supervisory authority*) si è espresso il Gruppo di lavoro articolo 29 per la protezione dei dati che il 13 dicembre 2016 ha adottato le "*Guidelines for identifying a controller or processor's lead supervisory authority*".

([28]) La disciplina del "meccanismo di coerenza" è contenuta nella sezione II del capo VII del regolamento. In particolare, l'art. 63 dispone che "al fine di contribuire all'applicazione coerente del presente regolamento in tutta l'Unione, le autorità di controllo cooperano tra loro e, se del caso, con la Commissione mediante il meccanismo di coerenza stabilito nella presente sezione".

([29]) Ai sensi dell'art. 79, comma 2°, infatti, le azioni nei confronti del titolare del trattamento o del responsabile del trattamento "sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri".

([30]) Il regime di responsabilità del titolare o del responsabile del trattamento è disciplinato all'art. 82, ove si precisa al comma 2° che "un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento" e al comma 3° che "il titolare del trattamento o il

Estremamente elevate le sanzioni amministrative che possono giungere fino al 4% del fatturato, rendendo così la nuova disciplina in materia di protezione dei dati personali ben più efficace dell'attuale.

5.1. *Le novità più rilevanti. Il nuovo approccio al rischio. Il principio di* accountability.

Fra le più rilevanti novità concernenti la disciplina sostanziale, ribadite le considerazioni derivanti dalla scelta dello strumento regolamentare appena svolte, si segnala il nuovo approccio al rischio dettato dal legislatore europeo, basato sul principio di *accountability*.

Come è noto, il problema da affrontare è quello delle misure di sicurezza che devono essere adottate a protezione dei dati personali per evitare o ridurre i rischi di accesso e divulgazione dei dati non autorizzati e i rischi di perdita e distruzione degli stessi.

Secondo il reg. UE 2016/679 [31], è il titolare del trattamento di dati personali a dovere valutare le misure tecniche e organizzative da adottare sulla base della natura dei dati, dell'oggetto, delle finalità di trattamento. Si tratta di misure non soltanto tecnologiche ma anche organizzative, dal momento che l'unico modo efficace di affrontare il problema della sicurezza dell'informazione è quello che ne comporta una visione integrata: informatica, giuridica e organizzativa. Occorre quindi che sulla sicurezza convergano più professionalità e più competenze – anche organizzative e legali – e che il problema non sia affrontato come problema di esclusiva competenza del responsabile del settore informatico.

---

responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile".

[31] L'art. 32, a tal proposito, dispone: "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati".

La sicurezza deve garantire la protezione dei dati in ciascuna delle singole operazioni del trattamento. La sicurezza è un concetto dinamico e relazionale, da rapportarsi alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati personali oggetto di trattamento ed alle specifiche caratteristiche delle operazioni di trattamento compiute.

Dunque sta al titolare individuare le misure di sicurezza da adottare dopo avere valutato la natura dei dati, il contesto, i rischi, i danni potenziali, i costi e lo stato dell'arte. Avendo definito le misure di sicurezza da adottare, il titolare deve compiere un'attività di continuo monitoraggio, per verificare che esse siano proporzionate e adeguate ai rischi, anch'essi in continuo mutamento. Occorre dunque una complessa attività di valutazione (tecnica, giuridica e organizzativa), un'analisi dei rischi e dei costi, una scelta sulle misure di sicurezza da adottare, l'istituzione di un presidio, l'emanazione di *policy* interne e quindi un'attività di monitoraggio continuo. Tutto ciò deve essere anche adeguatamente formalizzato e il titolare non soltanto deve attuare la normativa vigente, ma anche essere in grado di dimostrarlo.

Viene così adottato il principio dell'*accountability* (32), tradotto come "principio di rendicontazione" o "di responsabilità" e consistente nell'obbligo di conformarsi e di dimostrare (33).

Il Gruppo di lavoro articolo 29 per la protezione dei dati ha esaminato l'approccio alla protezione dei dati basato sul principio dell'*accountability* (34) nel parere 3/2010.

Il termine *accountability* può essere tradotto con responsabilità e, insieme, prova della responsabilità. Il titolare del trattamento deve essere in grado di dimostrare che ha adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi, analoghi a quelli utilizzati in Italia nell'applicazione del d.lgs. 8 giugno 2001, n. 231.

---

(32) Ho approfondito il tema dell'*accountability* nel mio *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, cit., p. 289 ss.

(33) Il concetto di *accountability* è già presente dal 1980 nelle Linee guida della OECD, (*Organisation for Economic Cooperation and Development*), in base alle quali: "*A data controller should be accountable for complying with measures which give effect to the [material] principles stated above*". Nell'ordinamento canadese il principio è menzionato nel *Personal Information Protection and Electronic Documents Act* .

(34) Sull'*accountability* si segnala il ruolo trainante del progetto "*Accountability-Based Privacy Governance*" promosso da The Centre for Information Policy Leadership che ha coinvolto circa 60 partecipanti internazionali, fra i quali Garanti, industrie, e accademici e al quale chi scrive ha avuto l'onore di partecipare.

Il termine "*accountability*" è tradotto nel citato parere 3/2010 del Gruppo di lavoro articolo 29 per la protezione dei dati con l'espressione "principio di responsabilità". Tuttavia, proprio in ragione della complessità della parola e dell'ampiezza dei significati e delle conseguenze cui può riferirsi si ritiene preferibile continuare ad utilizzare il termine originario "*accountability*", invece che la traduzione "principio di responsabilità". La difficoltà di comprendere il concetto di *accountability* dipende, in parte, dalle origini del concetto stesso, che nasce nella cultura anglosassone.

Come si afferma nel parere 3/2010 del Gruppo di lavoro articolo 29 per la protezione dei dati, *accountability* è un termine che può essere tradotto in molti modi diversi, fra i quali: responsabilità, affidabilità, assicurazione, obbligo di rendicontare, attuazione dei principi concernenti il trattamento dei dati personali. Queste possibili traduzioni chiariscono un aspetto dell'*accountability* e alcune conseguenze della stessa.

è necessario evidenziare che l'*accountability* è un meccanismo a due livelli.

L'*accountability* può basarsi su requisiti di base, normativamente posti, i quali sono vincolanti per tutti i titolari di trattamento, come pure su un sistema volontario.

Come precisa il parere 3/2010, "l'architettura giuridica dei meccanismi di responsabilità prevedrebbe due livelli: il primo livello sarebbe costituito da un obbligo di base vincolante per *tutti* i responsabili *(N.d.A.: titolari)* ([35]) del trattamento. Tale obbligo comprenderebbe due elementi: l'attuazione di misure e/o procedure, e la conservazione delle relative prove. Questo primo livello potrebbe essere integrato da disposizioni specifiche. Il secondo livello includerebbe sistemi di responsabilità di natura volontaria eccedenti le norme di legge minime, in relazione ai principi fondamentali di protezione dei dati (tali da fornire garanzie più elevate di quelle prescritte dalla normativa vigente) e/o in termini di modalità di attuazione o di garanzia dell'efficacia delle misure (norme di attuazione eccedenti il livello minimo)".

Evidentemente, l'*accountability* assume caratteristiche differenti nei due diversi casi.

Essa può essere considerata come un modo di formalizzare e proceduralizzare l'autonomia nei limiti che sono stati riconosciuti dalla Direttiva

---

([35]) Il termine "*data controller*" è reso nella versione italiana del parere 3/2010 con "responsabile". Il termine non pare corretto: il soggetto, secondo la legge italiana, responsabile dell'applicazione delle previsioni del Codice in materia di protezione dei dati personali, e in particolare dell'adozione di tutte le misure di sicurezza, è il titolare di trattamento.

e dalle normative nazionali. È un modo di creare una procedura, con un tipico approccio anglosassone, dove c'è l'autonomia.

Come si afferma nel parere 3/2010 del Gruppo di lavoro articolo 29 per la protezione dei dati sul principio dell'*accountability*, la nuova disposizione sull'*accountability* avrebbe lo scopo di promuovere l'adozione di misure concrete e pratiche, in quanto trasformerebbe i principi generali della protezione dei dati in politiche e procedure concrete definite al livello del responsabile del trattamento, nel rispetto delle leggi e dei regolamenti applicabili. Il titolare del trattamento dovrebbe anche garantire l'efficacia delle misure adottate e dimostrare, su richiesta, di aver intrapreso tali azioni. Quindi, come si è affermato, previsione della responsabilità e prova delle misure adottate per fare fronte alla responsabilità.

Secondo il Gruppo di lavoro articolo 29 per la protezione dei dati, due sono gli elementi principali:

"(i) la necessità che il responsabile *(N.d.A.: titolare)* del trattamento adotti misure appropriate ed efficaci per attuare i principi di protezione dei dati;

(ii) la necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci. Pertanto, il responsabile *(N.d.A.: titolare)* del trattamento deve fornire la prova di quanto esposto al punto (i)".

In relazione alla verifica dei modelli procedurali, tecnici e organizzativi adottati, ampio spazio è lasciato nel Regolamento alla certificazione, anche da parte di soggetti esterni.

E dunque strettamente collegata al principio dell'*accountability* è la previsione di meccanismi di certificazione della conformità delle misure adottate alla legge vigente ([36]).

Ancora, nell'ambito dell'attività di valutazione delle misure di sicurezza da adottarsi sono da ricondursi la valutazione di impatto sulla protezione dei dati, disciplinata dall'art. 35, e il *prior checking* disciplinato dall'art. 36.

La valutazione di impatto preventiva consiste nella valutazione dei trattamenti e dei rischi, della necessità dei trattamenti stessi e infine nell'individuazione di misure di sicurezza adeguate. Qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presentereb-

---

([36]) In particolare, con riferimento ai meccanismi di certificazione, l'art. 32, comma 3° precisa che "l'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo".

be un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio, il titolare del trattamento, prima di procedere al trattamento, deve consultare l'autorità per la protezione dei dati personali.

Ancora, nella valutazione e nell'adozione di misure volte a contenere il rischio possono essere ricondotti l'approccio basato sui metodi rispettivamente noti come *privacy by design* e *privacy by default*, di cui all'art. 25, che prevedono specificamente l'adozione di misure di pseudonimizzazione e minimizzazione del trattamento dei dati, nonché di protezione dei dati con riguardo all'accesso (37).

Nell'ambito di un nuovo approccio alla sicurezza, va segnalato l'obbligo, in parte già presente nella legislazione italiana, della *data breach notification*. Nel caso sia avvenuta una violazione dei dati personali, il titolare ha l'obbligo di notificarlo all'Autorità Garante e all'interessato, ai sensi dell'art. 33 e seguenti. Questa notificazione si aggiunge a quelle già previste dalla normativa europea e italiana in altri settori. Il regolamento eIDAS, infatti, impone ai prestatori di servizi fiduciari di notificare all'organismo di vigilanza e agli altri enti interessati, tra cui l'ente nazionale competente per la sicurezza delle informazioni (ENISA) e l'autorità di protezione dei dati, tutte le violazioni della sicurezza o le perdite di integrità che abbiano un impatto significativo sui servizi fiduciari prestati o sui dati personali custoditi (art. 19). Si conforma in tal senso anche la Dir. 2016/148/UE, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, che prevede obblighi di notifica in capo agli operatori di servizi essenziali e ai fornitori di servizi digitali nei confronti dell'autorità competente, designata ai sensi della Direttiva, o del CSIRT in caso di incidenti aventi un impatto rilevante

---

(37) Nello specifico, l'art. 25, comma 1° dispone: "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati". Inoltre, ai sensi del comma 2° "il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica".

sulla continuità dei servizi essenziali prestati (artt. 14 e 16). In particolare la Direttiva precisa che "in molti casi gli incidenti compromettono dati personali. Al riguardo è opportuno che le autorità competenti e le autorità responsabili della protezione dei dati collaborino e si scambino informazioni su tutti gli aspetti pertinenti per affrontare le violazioni ai dati personali determinate dagli incidenti" ([38]). A livello nazionale si segnalano invece gli obblighi di notifica previsti espressamente dall'art. 52-*ter* del testo unico bancario (t.u.b.) ([39]) e dalla circolare della Banca d'Italia n. 285 del 17 dicembre 2013 ([40]), che dispongono l'obbligo di comunicare tempestivamente alla Banca centrale europea o alla Banca d'Italia i gravi incidenti di sicurezza informatica.

Infine, nell'ambito del presidio del rischio, anche se la sua funzione non si esaurisce in questo ambito, va inquadrata la nuova figura del *data protection officer*, disciplinato dall'art. 37 e seguenti, caratterizzato da competenza specialista ed ampia autonomia, che riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento. Questi, nello svolgere la propria attività, deve considerare "debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo" ([41]).

Si tratta di un soggetto che è incaricato di vigilare sul rispetto della normativa in materia di *privacy* e di fungere da punto di contatto con l'autorità di controllo ([42]).

Questa figura era già prevista dalle disposizioni normative nazionali di diversi Stati membri, fra cui Germania, Svezia, Paesi Bassi, Francia e Lussemburgo.

([38]) 63°considerando Dir. 2016/1148/UE del Parlamento europeo e del Consiglio, del 6 luglio 2016, "recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione".

([39]) D.lgs. 1° settembre 1993, n. 385, "Testo unico in materia bancaria e creditiza", aggiornato al d.lgs. 14 novembre 2016, n. 233.

([40]) Titolo IV, sezione IV, paragrafo 6 della Circolare della Banca d'Italia n. 285 del 17 dicembre 2013, "Disposizioni di vigilanza per le banche", aggiornata da ultimo il 2 novembre 2016.

([41]) Così art. 39, comma 2°.

([42]) La figura del *privacy officer* è illustrata dal Gruppo di lavoro articolo 29 per la protezione dei dati nel "*Report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union*".

Più recentemente lo stesso Gruppo di lavoro articolo 29 per la protezione dei dati, al fine di agevolare l'individuazione del *data protection officer*, ha adottato, il 13 dicembre 2016, le "*Guidelines on Data Protection Officers ('DPO')*".

5.2. *Il criterio di ragionevolezza.*

L'influenza del pensiero giuridico maturato nella cultura di *common law* è palese non soltanto nel nuovo approccio al rischio basato sul principio della *accountability* e sul conseguente modello di responsabilità, ma anche nella introduzione del criterio di ragionevolezza. Il termine "ragionevole" e il termine "ragionevolmente" ricorrono frequentemente nel regolamento: a partire dall'individuazione dei dati anonimi del considerando n. 26 [43] fino all'art. 17 sul diritto all'oblio [44] e alle disposizioni in materia di sicurezza già citate [45].

5.3. *Ambito di applicazione territoriale.*

Fra le disposizioni più rilevanti quelle dell'art. 3, commi 1° e 2° ove si dispone: "Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:

a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure

b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione".

---

[43] Il 26° considerando, infatti, recita "(…) Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici".

[44] Si fa riferimento all'art. 17, comma 2°, il quale prevede che "il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali".

[45] Si fa riferimento alle disposizioni di cui agli artt. 32, 33 e 34.

Come precisato nei considerando n. 22, 23 e 24 il legislatore europeo intende affermare l'applicabilità del Regolamento europeo anche nel caso di trattamento dei dati personali degli interessati che si trovano nell'Unione ad opera di un titolare del trattamento o di un responsabile del trattamento non stabilito nell'Unione sia soggetto al Regolamento.

In questo senso milita la giurisprudenza della Corte di Giustizia europea con molte decisioni (46) fra le quali le più note: quelle relative ai casi *Google* e *Schrems*.

In estrema sintesi, la Corte, anticipando il Regolamento, afferma l'applicabilità della normativa europea anche nel caso in cui i titolari di trattamento dei dati personali siano soggetti non europei e i dati vengano trattati prevalentemente fuori dall'Europa.

La Corte europea si riappropria e consolida la posizione volta ad affermare l'applicazione del diritto europeo al trattamento dei dati personali degli europei. Si tratta di indirizzi profondamente politici in cui la Corte orgogliosamente sceglie cultura, principi e diritto europeo.

Lo strumento tecnico è costituito dall'interpretazione estensiva della nozione di "stabilimento".

Resta da verificare l'applicazione concreta ed effettiva di questa disposizione e, in particolare, la sua applicazione da parte dei giudici extraeuropei. Tuttavia, ancora una volta, appare evidente, che la protezione dei dati personali costituisca un tema politico di grande rilevanza, in cui gli interessi economici relativi al bene "informazione" sono sempre più evidenti.

5.4. *Il necessario bilanciamento di interessi.*

Il nuovo Regolamento pone l'accento sull'equilibrio degli opposti interessi e considera il diritto alla protezione dei dati personali necessariamente oggetto di bilanciamento. Il considerando n. 4 testualmente recita: "Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ottemperanza al principio di proporzionalità". Lo stesso considerando cita "tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai

(46) Si rinvia al mio contributo, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in AA.VV., *La protezione transnazionale dei dati personali dai* "safe harbour principles" *al* "privacy shield", RESTA e ZENO ZENCOVICH (a cura di), Roma, 2016.

trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica".

In questo senso, già alcune decisioni della Corte di giustizia, tra cui *Promusicae* (47), *Volker und Markus Schecke e Eifert* (48) e *ASNEF e FECEMD* (49), benché più recentemente, come si è illustrato, la Corte abbia fatto prevalere il diritto alla protezione dei dati personali sugli altri diritti.

Il considerando riporta alla mente alcune affermazioni della Corte di Cassazione italiana, in particolare quella contenuta nella sentenza n. 10280/2015 della Sezione III della Corte di Cassazione, ove si afferma che il diritto alla protezione dei dati personali, qualificato come pretesa ad esigere una corretta gestione dei propri dati personali, pur rientrando nei diritti fondamentali della persona, non è un "*totem* al quale possano sacrificarsi altri diritti altrettanto rilevanti sul piano costituzionale" e, conseguentemente, la disciplina in materia "va coordinata e bilanciata da un lato con le norme che tutelano altri e *prevalenti* diritti (tra questi, l'interesse pubblico alla celerità, trasparenza ed efficacia all'attività amministrativa); dall'altro, con le norme civilistiche in tema di negozi giuridici".

(47) CGUE,C-275/06,*ProductoresdeMuìsicadeEspan?a(Promusicae)c.TelefoìnicadeEspan?a SAU*, 29 gennaio 2008, cfr. punto 68.

(48) CGUE, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, 9 novembre 2010, cfr. punto 48.

(49) CGUE, cause riunite C-468/10 e C-469/10, *Asociacioìn Nacional de Establecimientos Financieros de Creìdito (ASNEF) e Federacioìn de Comercio Electroìnico y Marketing Directo (FECEMD) c. Administracioìn del Estado*, 24 novembre 2011, cfr. punto 43.