Alcune riflessioni a margine della nuova disciplina in materia di protezione dei dati personali di cui al Regolamento (UE) 2016/679[*]

SOMMARIO: 1. Un inquadramento di carattere generale del Regolamento (UE) 2016/679/UE. – 2. L'art. 8 della Carta dei diritti fondamentali dell'Unione europea nella giurisprudenza della Corte di giustizia. – 3. L'ambito di applicazione materiale del Regolamento (UE) 2016/679: la relazione tra il Codice *privacy* e il Regolamento generale e le problematiche inerenti alla loro coesistenza. – 3.1. L'applicazione del Regolamento (UE) 2016/679 in materia di diritto del lavoro. – 4. L'ambito di applicazione territoriale del Regolamento (UE) 2016/679. – 5. Il principio di responsabilizzazione del titolare del trattamento dei dati personali quale principale novità del nuovo Regolamento. – 6. Diritti nuovi e diritti "rafforzati" per l'interessato. – 7. Alcune considerazioni conclusive.

1. Un inquadramento di carattere generale del Regolamento (UE) 2016/679/UE

Nel settore digitale tutto si muove con un ritmo molto accelerato: un ritmo che si impone non solo a chi opera in questo campo, ma anche a chi è chiamato a stabilire le regole e a chi è tenuto ad assicurare che tali regole non soltanto siano rispettate, ma non finiscano per confliggere con principi giuridici che vengono enunciati e riconosciuti molto più lentamente e che, anche per questo motivo, sono ad esse gerarchicamente sovraordinati.

Con questa consapevolezza, l'Unione europea, ancora nel 2016, ha dato finalmente avvio a una riforma organica in tema di trattamento dei dati personali, ammodernando così regole divenute anacronistiche in un'epoca, oramai, a tutti gli effetti digitale. Una nuova realtà con cui anche il legislatore dell'Unione si è dovuto misurare, e lo ha fatto con non poca fatica per la complessità e la delicatezza dei

[*] Lo scritto riproduce, con modifiche e integrazioni, la relazione tenuta al convegno del 7 maggio 2018, *Il nuovo art. 4 Statuto Lavoratori. La tutela della riservatezza e il potere di controllo: discipline "antagoniste"?*, organizzato a Milano dalla Scuola Superiore della Magistratura, struttura territoriale di formazione decentrata. Non vi è, dunque, la pretesa di offrire un'analisi completa della nuova disciplina. D'altra parte, tale Regolamento, ben prima del 25 maggio 2018, data in cui esso è divenuto pienamente applicabile, è stato oggetto di svariati commenti, provenienti dall'accademia e dal mondo professionale, che hanno analizzato nel dettaglio le singole disposizioni di cui tale normativa si compone. Non è, invece, questo l'intento del presente contributo che, piuttosto, vuole mettere in luce alcuni aspetti che si presentano, a giudizio di chi scrive, problematici. Tenuto conto della natura del presente lavoro, i riferimenti bibliografici sono, quindi, di carattere essenziale.

profili che entrano in gioco, spesso rappresentativi di interessi ugualmente meritevoli di tutela anche se, almeno in apparenza, talvolta in conflitto fra loro. I dati personali, infatti, rappresentano una componente essenziale dell'identità di ciascun individuo che va preservata con ogni mezzo, ma, aggiungo, entro alcuni precisi confini, così che l'interesse privato e l'interesse pubblico possano pacificamente convivere.

Di certo, negli ultimi anni si è assistito a una crescita esponenziale nella quantità, qualità e diversità delle attività di trattamento dei dati personali. Per questo motivo, la creazione di un mercato unico digitale rappresenta per l'Unione europea una delle molte sfide su cui concentrare i propri sforzi anche negli anni a venire, tenuto conto che ci troviamo in presenza di un settore non trascurabile anche sul piano economico, dal momento che il suo contributo alla crescita del prodotto interno lordo europeo è stimato intorno ai cinquecentoventi miliardi di euro. Anche per tale motivo, la Commissione Juncker, presentando nel maggio del 2015 la sua agenda per il mercato unico digitale, ha previsto un piano di lavoro particolarmente ambizioso, basato su tre pilastri fondamentali e composto da sedici azioni, non tutte tradotte ancora in atti normativi.

Fra questi spicca per complessità e rilevanza il Regolamento (UE) 2016/679[1] del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito, "Regolamento generale" o "Regolamento"), che trae origine da una proposta della Commissione del 25 gennaio 2012[2] e, come si è detto, è divenuto direttamente e integralmente applicabile a partire dal 25 maggio 2018, dunque a circa due anni dalla sua entrata in vigore.

Questo Regolamento generale si inserisce in un pacchetto di riforme che sono destinate ad innovare profondamente il quadro normativo europeo in tema di tutela dei dati personali.

Infatti, si ricorda che, insieme al Regolamento generale, sono entrate in vigore due direttive: la direttiva (UE) 2016/680[3] del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati che abroga la decisione quadro 2008/977/GAI del Consiglio e la direttiva (UE) 2016/681[4] del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale

[1] In *GUUE* L 119 del 4.5.2016, p. 1.

[2] Proposta di Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (Regolamento generale sulla protezione dei dati) COM(2012)11 def.

[3] In *GUUE* L 119 del 4.5.2016, p. 89.

[4] *Ibidem*, p. 132.

nei confronti dei reati di terrorismo e dei reati gravi, il cui termine di recepimento negli ordinamenti nazionali era, rispettivamente, il 6[5] e il 25[6] maggio di quest'anno.

La Commissione ha previsto anche l'adozione di un Regolamento in materia di *e-privacy* che andrà a sostituire l'attuale direttiva 2002/58/CE con l'obiettivo di estendere, in quanto *lex specialis*, l'ambito di applicazione della disciplina sulla tutela dei dati personali anche ai trattamenti legati allo scambio di e-mail e di messaggi, comunicazioni via *social network* e a tutto quanto rientri nella definizione di comunicazione elettronica. La proposta di direttiva[7] è attualmente in discussione al Consiglio e l'auspicio della Commissione è che il regolamento possa venire approvato entro la fine della legislatura europea.

Questo nuovo quadro giuridico di cui si sta dotando l'Unione europea trae la sua origine dal "Programma di Stoccolma — Un'Europa aperta e sicura al servizio e a tutela dei cittadini"[8] in cui il Consiglio europeo ha invitato la Commissione a valutare il funzionamento degli strumenti giuridici dell'Unione in materia di protezione dei dati e a presentare, se quest'ultima lo avesse ritenuto necessario, iniziative a carattere legislativo o anche prive di tale natura. Nella sua risoluzione sul programma di Stoccolma[9], il Parlamento europeo ha accolto con favore la proposta relativa ad un quadro giuridico completo in materia di protezione dei dati nell'UE, mentre la Commissione, nel piano d'azione per l'attuazione di tale programma[10], ha sottolineato la necessità di assicurare l'applicazione sistematica del diritto fondamentale alla protezione dei dati personali nel contesto di tutte le politiche europee.

In una successiva comunicazione del 2010, dal titolo "Un approccio globale alla protezione dei dati personali nell'Unione europea"[11], la Commissione ha sostenuto che l'Unione europea avesse bisogno di una politica più completa e coerente in tema di protezione dei dati personali.

La *ratio* di una tale riforma organica è da rinvenirsi nella necessità di introdurre specifiche regole in grado di rispondere alle nuove sfide che la tecnologia e il suo evolvere pongono rispetto al diritto alla tutela dei dati personali[12]. Si avvertiva

---

[5] La direttiva (UE) 2016/680 è stata recepita nell'ordinamento italiano con il d.lgs n. 51 del 18.5.2018, in *GU* Serie Generale n. 119 del 24.5.2018, in vigore a partire dall'8.6.2018.

[6] La direttiva (UE) 2016/681 è stata recepita nell'ordinamento italiano con il d.lgs n. 53 del 21 maggio 2018, n in *GU* Serie Generale n. 120 del 25.5.2018, in vigore a partire dal 9.6.2018.

[7] COM(2017)10 def.

[8] In *GUUE* 115 del 4.5.2010, p. 1.

[9] Risoluzione del Parlamento europeo sulla comunicazione della Commissione al Parlamento europeo e al Consiglio dal titolo "Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini - Programma di Stoccolma", adottata il 25.11.2009 (P7_TA (2009) 0090).

[10] COM(2010) 171 def.

[11] COM(2010) 609 def.

[12] Cfr. Commissione europea COM(2010) 11 def. del 25.1.2012, *Proposta di Regolamento del Parlamento europeo e del Consiglio concernente la tutela della persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati*;

allora, dunque, l'esigenza di adeguare l'impianto normativo al nuovo contesto tecnologico al fine di instaurare un clima di fiducia negli ambienti *on line* e permettere al tempo stesso un continuo sviluppo economico[13], fondato su applicazioni tecniche innovative.

2. L'art. 8 della Carta dei diritti fondamentali dell'Unione europea nella giurisprudenza della Corte di giustizia

Il Regolamento generale di fatto codifica alcune pronunce della Corte di giustizia in merito all'applicazione, anche in un contesto digitale, delle regole sulla *privacy*[14].

L'*acquis communautaire* in materia di protezione dei dati personali ha, infatti, visto quale fondamentale attore la Corte di giustizia la quale, ancora prima dell'entrata in vigore della direttiva 95/46/CE che il Regolamento (UE) 2016/679 sostituisce, ha permesso di edificare in via pretoria un diritto alla protezione dei dati personali tale da garantire una tutela elevata e il più possibile adeguata all'evoluzione tecnologica, anche quando la stessa direttiva 95/46/CE si è rivelata inadatta o incompleta.

Grazie a questa giurisprudenza evolutiva in materia di protezione dei dati personali, anche a livello di Unione europea, la tutela della *privacy* ha assunto nel tempo connotazioni diverse, passando dall'essere considerata quale eccezione alle libertà economiche sancite dai Trattati, per giungere oggi, ancor prima dell'applicazione del Regolamento, a una configurazione orientata sui diritti fondamentali[15].

---

nonché Corte giust., sentenza del 13.5.2014, causa C-131/12, *Google Spain SL, Google Inc. c. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez*, ECLI:EU:C:2014:317, pt. 80.

[13] V. Commissione europea COM(2010) 11 def., cit., spec. p. 1, ove la Commissione nell'illustrare il contesto della Proposta afferma che gli «incalzanti sviluppi tecnologici hanno allontanato le frontiere della protezione dei dati personali. La portata della condivisione e della raccolta di dati è aumentata in modo vertiginoso: la tecnologia attuale consente alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività e, sempre più spesso, gli stessi privati rendono pubbliche sulla rete mondiale informazioni personali che li riguardano».

[14] Cfr. M. BASSINI, *La svolta della* privacy *europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quaderni costituzionali*, fascicolo 3, 2016, p. 587 ss. Cfr. in merito all'attivismo della Corte di giustizia in materia di tutela dei dati personali nel nuovo contesto di sviluppo tecnologico, O. POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla* privacy *digitale*, in *Federalismi.it*, 24.11.2014.

[15] Cfr. anche COM(2018) 43 def. del 24.1.2018, Comunicazione della Commissione al Parlamento europeo e al Consiglio, Maggiore protezione, nuove opportunità – Orientamenti della Commissione per l'applicazione diretta del regolamento generale sulla protezione dei dati a partire dal 25 maggio 2018, spec. p. 1 ove si afferma che «il

A questa trasformazione ha contribuito il Trattato di Lisbona con il nuovo articolo 16 del TFUE[16], il quale afferma nel primo paragrafo che «Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano», e con le modifiche apportate all'art. 6 del TUE con cui alla Carta dei diritti fondamentali dell'Unione europea è stato riconosciuto il medesimo valore giuridico dei Trattati[17].

In particolare, l'articolo 8 della Carta rappresenta il punto di arrivo di un processo di codificazione e costituzionalizzazione del diritto europeo alla *privacy*[18] e al tempo stesso costituisce la pietra angolare di questo nuovo impianto normativo di cui l'Unione si è dotata[19]. Con l'art. 8 della Carta tale diritto, da una dimensione di carattere essenzialmente negativo (codificata, oltre che dalla CEDU all'art. 8, dall'art. 7 della stessa Carta, nonché espressione del c.d. "*right to be alone*" poiché, come affermato ancora nel 1952 da un giudice della Corte Suprema degli Stati Uniti, «il diritto di essere lasciati in pace è di fatto l'inizio di ogni libertà»[20]), approda a una dimensione di carattere positivo, che si traduce nella tutela dei dati

---

regolamento rafforzerà la tutela del diritto dei cittadini alla protezione dei dati personali, riflettendone la natura di diritto fondamentale dell'Unione europea».

[16] Art. 16 TFUE (*ex* art. 286 TCE) il quale attribuisce al legislatore europeo la facoltà di adottare, mediante procedura legislativa ordinaria, una normativa relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e alla loro libera circolazione da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, affidando il rispetto di tali norme ad autorità indipendenti. V. F. PIZZETTI, *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, in (a cura di) P. BILANCIA, M. D'AMICO, *La nuova Europa dopo il Trattato di Lisbona*, 2009, p. 83 ss. e il commento di B. CORTESE, *Art. 16*, in (a cura di) A. TIZZANO, *Trattati dell'Unione europea*, Milano, 2014, p. 444 ss.

[17] Sul punto, v. S. CRESPI, *Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati*, in *Rivista Italiana di diritto pubblico comunitario*, 2015, p. 819 ss.

[18] V. O. POLLICINO, M. BASSINI, *Commento all' art. 8 CdfUE*, in (a cura di) R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI, *Carta dei diritti fondamentali dell'Unione europea*, p. 132 ss., spec. p. 135.

[19] Le Spiegazioni della Carta fanno espressamente menzione ai riferimenti normativi che hanno contribuito al processo di codificazione del diritto alla *privacy* nell'ordinamento dell'Unione europea: (*i*) l'art. 16 TFUE; (*ii*) la direttiva 95/46/CE, cit.; (*iii*) la Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale del 28 gennaio 1981 (ratificata da tutti gli Stati membri in quanto parti contraenti del Consiglio d'Europa); (*iv*) il regolamento (CE) n. 45/2001 concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati; (*v*) l'art. 8 CEDU.

[20] Cfr. il caso *Public Utilities Commission c. Pollak*, 343 U.S. 451, 467 (1952) e l'opinione del giudice William O. Douglas, dissenziente. Cfr. S.D. WARREN, L.D. BRANDEIS, *The right to privacy*, in *Harvard Law Review*, 1980, p. 193 ss. Gli autori affermano un diritto alla *privacy*, secondo un'accezione negativa, da intendersi quale *right to be alone* ossia il diritto al rispetto della vita privata e familiare, codificato nell'ordinamento europeo dall'art. 7 della Carta.

personali mediante la creazione di un insieme di regole e principi[21]. L'art. 8 della Carta, dunque, consente di costruire un sistema di controlli e contrappesi che va oltre il concetto di consenso e che permette il trattamento lecito dei dati, talvolta anche prescindendo da un'autorizzazione esplicita dell'interessato. I paragrafi 2 e 3 dell'articolo 8 della Carta precisano che tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge, che ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica, e, infine, che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente[22]. Tali prescrizioni mutuate dagli articoli 6, 7, 12, 14 e 28 della direttiva 95/46/CE sono parimenti codificate nel nuovo Regolamento.

Il ruolo della Corte di giustizia quale interprete del quadro normativo previsto dalla direttiva 95/46/CE e dall'art. 8 della Carta è emerso prepotentemente negli ultimi anni, in particolare in relazione all'evoluzione tecnologica. Basti citare la sentenza *Digital Rights Ireland* con la quale la Corte ha dichiarato invalida la direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, c.d. direttiva "*data retention*", sulla conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione[23].

A tale riguardo, la Corte ha osservato che, in considerazione, da un lato, dell'importante ruolo svolto dalla protezione dei dati personali nei confronti del diritto fondamentale al rispetto della vita privata e, dall'altro lato, della portata e della gravità dell'ingerenza in tale diritto che la direttiva comporta, fosse necessario il controllo di un giudice o di un ente amministrativo indipendente sull'utilizzo da parte delle autorità nazionali competenti dei dati personali per finalità di prevenzione o contrasto di reati[24].Secondo la Corte, la normativa dell'Unione

---

[21] V. O. POLLICINO, M. BASSINI, *Commento all'art. 8 CdfUE*, cit., spec. p. 136.

[22] Sentenza del 9.3.2017, C-398/15, *Manni*, ECLI:EU:C:2017:197.

[23] Corte giust., sentenza del 8.4.2014, cause riunite C-293/12 e C-594/12*, Digital Rights Ireland Ltd*, ECLI:EU:C:2014:238. Si noti peraltro che in tale pronuncia la Corte ha deciso per la prima volta nella storia del processo di integrazione europea di dichiarare nullo un atto di diritto derivato dell'Unione perché in contrasto con la Carta dei diritti fondamentali (articoli 7, 8 e 52, paragrafo 1), avendo il legislatore UE ecceduto i limiti imposti dal rispetto del principio di proporzionalità.

[24] Sul punto cfr. Corte giust. sentenza del 9.11. 2010, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke e Eifert*, ECLI:EU:C:2010:662, spec. pt. 47. Per un commento a tale pronuncia si veda E. DEGRAVE, *Arrêt "Volker und Markus Schecke et Eifert": le droit fondamental à la protection des données à caractère personnel et la transparence administrative*, in *Journal de droit européen*, 2011, p. 97; D. DERO-BUGNY, *Protection des personnes physiques à l'égard du traitement des données à caractère personnel*, in *Journal du droit int.*, 2011, p. 492; I. ANDOULSI, *L'arrêt de la Cour du 9 novembre 2010 dans les affaires jointes Volker und Markus Schecke GBR et Hartmut Eifert contre Land d'Hessen (C-92/09 et C-93/09): une reconnaissance jurisprudentielle du droit fondamental à la protection des données personnelles?*, in *Cahiers de droit européen*, 2011, p. 471. Si aggiunga che l'accesso delle autorità nazionali competenti ai dati di natura personale costituisce di per sé un'ingerenza supplementare in tali diritti fondamentali. In questo senso, con riferimento all'applicazione dell'art. 8 della Convenzione europea, cfr. le

avrebbe dovuto prevedere regole chiare e precise con cui stabilire strumenti idonei a proteggere efficacemente i dati personali dal rischio di abusi nonché da eventuali accessi e usi illeciti nelle attività di trattamento[25].

Sulla scia della sentenza *Digital Rights Ireland* si pone la pronuncia *Google Spain*[26] in cui la Corte, disattendendo le conclusioni dell'Avvocato generale Jääskinen[27], ha riconosciuto per la prima volta l'esistenza nell'ordinamento dell'Unione del cosiddetto "diritto all'oblio".

Più precisamente, in quest'ultima pronuncia, interpretando alcune delle disposizioni contenute nella direttiva 95/46/CE, lette alla luce degli articoli 7 e 8 della Carta, la Corte ha affermato l'esistenza di un diritto del singolo interessato a chiedere, in presenza di determinate condizioni, al gestore del motore di ricerca prima, e alle autorità competenti poi, l'eliminazione dei *link* verso pagine *web* pubblicate da terzi, dall'elenco dei risultati che appare a seguito di una ricerca effettuata a partire dal nome di tale soggetto, partendo dalla considerazione che «[l']attività di un motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di internet secondo un determinato ordine di preferenza, deve essere qualificato come trattamento di dati personali, e che il gestore di detto motore di ricerca deve essere considerato come il responsabile del trattamento»[28].

---

sentenze della Corte di Strasburgo del 26 marzo 1987, *Leander* c. *Svezia*, serie A n. 116, § 48, e del 4 maggio 2000, *Rotaru* c. *Romania* [GC], n. 28341/95, par. 46, CEDU 2000-V.

[25] Corte giust., sentenza *Digital Rights Ireland Ltd*, cit., pt. 54.

[26] Cfr. Corte giust., sentenza del 13.5.2014, causa C-131/12, *Google Spain*, ECLI:EU:C:2014:317; Corte giust., sentenza *Digital Rights Ireland Ltd*, cit.

[27] Cfr. Conclusioni dell'Avvocato generale Jääskinen presentate il 25.06.2013, causa C-131/12, *Google Spain*, ECLI:EU:C:2013:424, spec. pt. 108-110, ove l'Avvocato generale ha affermato di non ritenere sussistente, ai sensi della direttiva 95/46/CE, «un diritto generale all'oblio nel senso che una persona interessata abbia il diritto di limitare o di porre fine alla diffusione di dati personali che consideri nocivi o contrari ai propri interessi. Sono lo scopo del trattamento e gli interessi da esso tutelati, confrontati con quelli della persona interessata, e non le preferenze di quest'ultima, i criteri da applicare allorché i dati vengono trattati senza il consenso della stessa. Di per sé, una preferenza soggettiva non costituisce un motivo preminente e legittimo ai sensi dell'articolo 14, lettera a), della direttiva».

[28] V. Corte giust., sentenza *Google Spain*, cit., punto 41. Nella specie, la Corte ha affermato la preminenza del diritto alla protezione dei dati personali alla luce del fatto che (*i*) il Signor González, cittadino spagnolo con domicilio in Spagna, non rivestiva un ruolo pubblico; (*ii*) l'informazione messa a disposizione del pubblico, ovvero la notizia del pignoramento e della vendita all'asta di proprietà immobiliari del Signor González non rivestiva interesse pubblico, bensì si trattava di un'informazione di carattere sensibile per la vita privata dell'interessato; (*iii*) la pubblicazione di tale informazione era stata effettuata sedici anni prima e pertanto non ricorreva alcun presupposto per affermare il diritto di informazione del pubblico, al contrario risultava illegittimo e in violazione del diritto alla protezione dei dati personali il fatto che i link a detta notizia figurassero ancora tra le informazioni che Google riportava in merito al Signor González.

Anche in questa pronuncia la Corte ha operato, dunque, un bilanciamento fra interessi contrapposti, assegnando la prevalenza al diritto alla protezione della vita privata e dei dati personali, non già rispetto all'interesse pubblico alla repressione dei crimini e alla lotta contro il terrorismo come avvenuto nella sentenza *Digital Rights Ireland*, bensì con riguardo alla libertà di informazione e alla libertà economica dei fornitori di servizi elettronici. Per tale via, per la prima volta, la Corte ha riconosciuto che anche il diritto alla protezione dei dati personali possa assumere una capacità limitativa rispetto ad altri diritti fondamentali della persona. Questa giurisprudenza è oggi codificata nel Regolamento all'art. 17 che sancisce, per l'appunto, il cosiddetto "diritto ad essere dimenticati".

In tema di trasmissione, trattamento e conservazione dei dati personali da parte di autorità pubbliche di Paesi terzi, va segnalata la sentenza della Corte *Schrems* (o, per usare un termine più evocativo, "Facebook") del 6 ottobre 2015.[29].

3. L'ambito di applicazione materiale del Regolamento (UE) 2016/679: la relazione tra il Codice *privacy* e il Regolamento generale e le problematiche inerenti alla loro coesistenza

Il Regolamento (UE) 2016/679, come si è già ricordato, sostituisce una direttiva e le caratteristiche stesse di questo atto legislativo fanno sì che, in un'ottica di sviluppo del mercato interno, esso costituisca il miglior strumento per il raggiungimento di un livello minimo di tutela dei dati personali che sia equivalente in tutti gli Stati membri. Da qui, la conformità di tale atto con il principio di sussidiarietà, sancito dall'art. 5 del TUE, nonché con il principio di proporzionalità previsto dalla medesima disposizione. Sebbene vada ricordato che sono stati presentati pareri motivati, nel quadro del protocollo n. 2 sull'applicazione dei principi appena evocati, allegato ai Trattati, dalla Camera dei rappresentanti belga, dal Bundesrat tedesco, dal Senato francese, dal Parlamento svedese e anche dalla nostra Camera dei deputati[30], in cui si era lamentata la mancata conformità del progetto di atto legislativo al principio di sussidiarietà.

L'applicazione del Regolamento non implica, tuttavia, un'uniformazione completa delle legislazioni degli Stati membri in materia, in quanto talora chiede, talora consente al legislatore nazionale di introdurre varie norme di dettaglio, con il fine di rendere operativa la disciplina, e di carattere settoriale, potendo stabilire deroghe, positive e negative, esenzioni e limitazioni di parte speciale. Tali norme dovranno in ogni caso essere adottate dagli Stati membri nel rispetto del principio di leale cooperazione, implicitamente richiamato dall'art. 16, par. 2 del TFUE, che,

[29] Sentenza del 6.10.2015, causa C-362/14, *Schrems*, ECLI:EU:C:2015:650. Per un primo commento, cfr. F. ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal* Safe Harbour *al* Privacy Shield*)*, in *Rivista di diritto internazionale*, 2016, p. 690 ss.

[30] Cfr. http://ec.europa.eu/dgs/secretariat_general/relations/relations_other/npo/docs/italy/2012/ com 20120011/com20120011_senato_opinion_it.pdf.

per l'appunto, vieta loro di adottare atti che possano mettere in pericolo l'attuazione o che siano contrari al diritto dell'Unione e ai suoi obiettivi.

Possiamo, quindi, parlare di un riordino normativo attuato dal Regolamento che impone, ma solo quanto ad alcuni profili, livelli omogenei di tutela in tutta l'Unione europea.

Un primo profilo rilevante rispetto all'applicazione del Regolamento è, dunque, che esso non si sostituisce o interamente assorbe la disciplina nazionale che, nel nostro ordinamento, è contenuta essenzialmente nel d.lgs. 196/2003, c.d. "Codice *privacy*". Gli Stati membri sono, infatti, chiamati a introdurre nel proprio ordinamento giuridico le misure necessarie per adattare la legislazione interna così da garantire la piena effettività ed efficacia del Regolamento stesso[31].

Dunque, da un lato il legislatore dell'UE ha inteso ricondurre il perimetro del suo intervento a profili generali e trasversali che attengono al cuore della materia, quali i fondamenti di liceità del trattamento, le condizioni del consenso, i diritti dell'interessato, il contenuto dell'informativa, la caratterizzazione delle varie figure che oggi intervengono nelle attività di trattamento dei dati (il titolare, il responsabile del trattamento e il responsabile della protezione dei dati), il principio di responsabilizzazione del titolare del trattamento, il ricorso alla pseudonimizzazione e alla cifratura dei dati come misure di garanzia, l'obbligo per il titolare del trattamento di notificare le violazioni all'autorità di controllo entro 72 ore dal momento in cui ne è venuto a conoscenza, le condizioni per il trasferimento dei dati verso Paesi terzi, dall'altro lato ha demandato al legislatore nazionale il compito di completare la disciplina in una dimensione sia orizzontale, prevedendo, ad esempio, le modalità procedurali per l'esercizio dei diritti, sia settoriale, con riferimento a diverse aree giuridiche che incidentalmente si intersecano con i dati personali.

Il Regolamento, infatti, consente agli Stati membri di regolare interi settori e di precisare ulteriormente l'applicazione delle norme in materia di protezione dei dati, anche sensibili, in ambiti specifici: l'amministrazione della giustizia, la medicina preventiva e la medicina del lavoro, la sanità pubblica, l'archiviazione nel pubblico interesse, la ricerca scientifica o storica o a fini statistici, l'accesso del pubblico ai documenti ufficiali, gli obblighi di segretezza e nei rapporti di lavoro e sicurezza sociale dove, va ricordato, il pilastro europeo dei diritti sociali (2017/C 428/09) stabilisce, anche, che: «I lavoratori hanno diritto alla protezione dei propri dati personali nell'ambito del rapporto di lavoro»[32].

Si aggiunga che l'ambito di applicazione materiale del regolamento è limitato. L'art. 2 prevede al primo paragrafo che esso «si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi». Il paragrafo 2 del medesimo articolo elenca i casi in cui il Regolamento non si applica, ossia in relazione a trattamenti di dati personali *a*) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione; *b*) effettuati dagli Stati membri

[31] Cfr. COM(2018) 43 def, cit., spec. p. 9 e ss. In questo documento si dà atto che solo Austria e Germania avevano al 24.1.2018 già implementato il Regolamento adattando la previgente disciplina nazionale.

[32] In *GUUE* C 428 del 13 dicembre 2017, p. 10.

nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE; *c*) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; *d*) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

Non sorprende certamente che sia escluso dal campo di applicazione del nuovo Regolamento il trattamento effettuato da una persona fisica per l'esercizio di attività a carattere esclusivamente personale e domestico (lett. c), che rappresenta di per sé una garanzia per l'individuo o il trattamento dei dati nel quadro della PESC o della cooperazione di polizia o giudiziaria in materia penale, essendo quest'ultimo disciplinato dalla direttiva 2016/680/UE. Invece, qualche problema interpretativo si pone rispetto a quanto previsto alla lett. a), ovvero la non applicazione del Regolamento per i trattamenti di dati personali effettuati per attività che non rientrino nell'ambito di applicazione del diritto dell'Unione.

Di questa disposizione, che, peraltro, era già presente nella direttiva 95/46/CE, si possono dare due letture diverse. La prima richiama una distinzione[33] ben nota agli studiosi del diritto UE fra fattispecie puramente interne e fattispecie in cui trova attuazione il diritto dell'Unione, così come previsto, sempre restando in tema di tutela dei diritti fondamentali, dall'art. 51 della Carta per delimitare il suo campo di applicazione.

Una tale interpretazione costringerebbe l'operatore e l'interprete a complesse analisi e valutazioni in considerazione del contesto in cui operano.

Un diverso trattamento si potrebbe avere anche nell'ambito dei rapporti fra il singolo e la pubblica amministrazione, a seconda del settore considerato.

La seconda lettura, l'unica che pare corretta, porta, invece, a ritenere il Regolamento comunque applicabile in tutti i casi in cui vengano in rilievo dati personali, a prescindere dalla cittadinanza dell'interessato, essendo l'espressione "ambito di applicazione del diritto dell'Unione" da intendersi come comprensiva di tutte quelle misure nazionali che presentino un collegamento anche solo funzionale con una disposizione del diritto dell'Unione (in questo caso rappresentata dall'art. 16 del TFUE), salvo si sia in presenza di attività che effettivamente esulino dal diritto dell'Unione, quali, come ci ricorda il *considerando* sedicesimo del Regolamento, quelle che riguardano la sicurezza nazionale. Anche se, per la verità, a questo proposito, non va dimenticato che i concetti di "sicurezza nazionale", "sicurezza interna dell'UE" e "sicurezza internazionale" tendono spesso a sovrapporsi, essendo obiettivi che devono essere necessariamente perseguiti tutti nel rispetto dei valori e dei principi sanciti dall'art. 2 TUE e dalla stessa Carta dei diritti fondamentali.

In ogni caso, non semplice appare il compito affidato al legislatore nazionale, il quale deve adeguare le norme interne al Regolamento e completare la disciplina entro la cornice di tale atto, assicurandone al contempo la coerenza.

---

[33] Per la definizione di "situazioni puramente interne" si veda, da ultimo, Corte giust., sentenza del 6.12.2012, *O. e S.*, C-356/11 e C-357/11, ECLI:EU:C:2012:776, pt. 43. Cfr. R. ADAM, A. TIZZANO, *Manuale di diritto dell'Unione europea*, Milano, 2017, p. 386.

A tale compito, il Governo italiano è stato chiamato dall'art. 13 della Legge 25 ottobre 2017, n. 163 (Legge di delegazione europea 2016-2017) [34] che gli chiede di modificare il decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto

[34] In *GU* n. 259 del 6.11.2017, il cui art. 13 precisa che: «1. Il Governo è delegato ad adottare, entro sei mesi dalla data di entrata in vigore della presente legge, con le procedure di cui all'articolo 31 della legge 24 dicembre 2012, n. 234, acquisiti i pareri delle competenti Commissioni parlamentari e del Garante per la protezione dei dati personali, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE. 2. I decreti legislativi di cui al comma 1 sono adottati su proposta del Presidente del Consiglio dei ministri e del Ministro della giustizia, di concerto con i Ministri degli affari esteri e della cooperazione internazionale, dell'economia e delle finanze, dello sviluppo economico e per la semplificazione e la pubblica amministrazione. 3. Nell'esercizio della delega di cui al comma 1 il Governo è tenuto a seguire, oltre ai principi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, anche i seguenti principi e criteri direttivi specifici: a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679; b) modificare il codice di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679; c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679; d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal regolamento (UE) 2016/679; e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse. 4. Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e ad essa si provvede con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente». Sul punto, il Governo non potrà non tener conto delle raccomandazioni formulate dalla Commissione in merito alla corretta implementazione del Regolamento. Cfr. COM(2018) 43 def., cit., spec. p. 9 e ss., ove la Commissione rammenta che: «È altresì vietato integrare il testo dei regolamenti nel diritto nazionale (per esempio ripetere le definizioni o i diritti dei singoli), a meno che tale integrazione sia strettamente necessaria ai fini della coerenza e per rendere le disposizioni nazionali comprensibili alle persone cui si applicano. La riproduzione del testo del regolamento parola per parola nella legge nazionale di precisazione è ammessa solo in circostanze eccezionali e giustificate e non può essere usata per inserire condizioni o interpretazioni aggiuntive al testo del regolamento. L'interpretazione del regolamento spetta agli organi giurisdizionali europei (giudici nazionali e, da ultimo, Corte di giustizia dell'Unione europea) e non ai legislatori degli Stati membri. Il legislatore nazionale pertanto non può copiare il testo del regolamento se non è necessario alla luce dei criteri forniti dalla giurisprudenza, né interpretarlo o inserire condizioni aggiuntive alle norme direttamente applicabili in virtù del regolamento. Se lo facesse, gli operatori nell'Unione si troverebbero di nuovo di fronte a un quadro frammentato e non saprebbero quali norme sono tenuti a rispettare».

necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel Regolamento 2016/679, abrogando le norme interne incompatibili, coordinando le disposizioni vigenti e quelle che saranno adottate con la normativa dell'Unione, prevedendo, se necessario, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali e, infine, adeguando, nell'ambito delle modifiche al Codice *Privacy*, il sistema sanzionatorio.

La prima versione dello schema di decreto legislativo approvata dal Consiglio dei Ministri lo scorso 21 marzo ha sollevato molte perplessità per il fatto di porsi in evidente contrasto con la delega ricevuta dal Governo. Tale versione, infatti, prevedeva, all'art. 101, l'abrogazione dell'intero d.lgs. 196 del 2003, sostituito dal nuovo decreto, ed una pressoché totale depenalizzazione degli illeciti, fatto salvo il caso di false dichiarazioni od ostacoli alle attività del Garante (art. 35).

L'ultima versione dello schema di decreto legislativo, sottoposta al vaglio della Commissione speciale per gli atti di Governo il 23 maggio 2018[35], invece, e più correttamente, si limita a prevedere una profonda e imponente revisione del Codice *Privacy*, abrogando le disposizioni incompatibili con il Regolamento e, al contempo, inserendone altre, necessarie a completare la disciplina.

Tale ultima versione, inoltre, limita i casi di depenalizzazione e ripropone una sezione penale, in cui figurano nuovi illeciti, come l'acquisizione fraudolenta di dati personali e la loro comunicazione e diffusione illecita quando sia coinvolto un rilevante numero di persone. Inoltre, viene previsto un regime transitorio per i procedimenti pendenti.

D'altra parte, nello stabilire il regime sanzionatorio, il legislatore nazionale deve tenere conto della giurisprudenza sui c.d. "vasi comunicanti"[36] della Corte di giustizia, richiamata anche dal *considerando* 149 del Regolamento, che, interpretando, in linea con i noti criteri Engel[37] elaborati dalla Corte EDU, il principio del *ne bis in idem*, codificato all'art. 50 della Carta dei diritti fondamentali dell'UE, esclude, in presenza di determinate condizioni, il cumulo tra sanzioni amministrative, specie se di entità significativa, e sanzioni penali, avendo le prime la stessa natura delle seconde[38].

---

[35] L'esame è poi stato rinviato ad altra seduta. Cfr. http://www.camera.it/leg18/1132?shadow_ primapagina=7722.

[36] Espressione utilizzata in questo contesto da L. BOLOGNINI, S*uperare una concezione fondamentalista della privacy". L'analisi della Bozza di riordino tra luci ed ombre*, in https://www.dimt.it, 13.4.2018.

[37] Stando a tali criteri, il carattere penale di una sanzione va valutato in base *a)* alla qualificazione giuridica dell'illecito nel diritto nazionale, *b)* alla natura dell'illecito, *c)* alla natura e severità à della sanzione.

[38] Il riferimento è alle sentenze della Corte di giustizia del 6.2.2013, causa C-617/10, *Åkerberg Fransson*, ECLI:EU:C:2013:105; del 5.6.2012, causa C-489/10, *Bonda*, ECLI:EU:C:2012:319; del 20.3.2018 nelle cause C- 524/15, *Menci*; C-537/16, *Garlsson Real Estate;* cause riunite C-596/16 e C- 597/16 *Di Puma* e *Consob*, rispettivamente, in ECLI:EU:C:2018:197; ECLI:EU:C:2018:193; ECLI:EU:C:2018:192. In tema, v., su tutti, B. NASCIMBENE, Ne bis in idem*, diritto internazionale e diritto europeo*, in *Eurojus.it*, 22.3.2018.

Il Regolamento si limita, peraltro, a consentire agli Stati membri di introdurre nel proprio ordinamento sanzioni penali, ma questa, che per l'appunto è solo una facoltà, va esercitata con molta cautela.

3.1. L'applicazione del Regolamento (UE) 2016/679 in materia di diritto del lavoro

Con riferimento allo schema di decreto, in attesa che venga approvato un testo definitivo, si vogliono richiamare alcune sue disposizioni che attengono, in particolare, ai profili giuslavoristici sia sul piano processuale sia sul piano sostanziale. A cominciare da quello che dovrebbe essere il nuovo articolo 140 *bis* del Codice della *privacy* il quale prevede il reclamo al Garante, ai sensi dell'articolo 77 del Regolamento, sempre come mezzo di tutela alternativo al ricorso all'autorità giudiziaria competente, ovvero quella ordinaria, secondo il rito del lavoro.

Lo schema di decreto introduce alcune modifiche all'articolo 10 del decreto legislativo 1° settembre 2011 n. 150.

Fra i profili innovativi, uno riguarda la competenza territoriale. Il nuovo comma 2 dell'art. 10, così modificato, prevede, infatti, in via alternativa la competenza del tribunale del luogo in cui il titolare del trattamento ha la residenza o la sede e del "tribunale del luogo di residenza dell'interessato".

Un'altra novità è contenuta nel comma 5 in base al quale l'interessato può dare mandato a un ente del terzo settore soggetto alla disciplina del decreto legislativo 3 luglio 2017, n. 117 di esercitare per suo conto l'azione, in conformità a quanto previsto dall'articolo 80 e dal *considerando* 147 del Regolamento.

Infine, il comma 9 prevede che, nei casi in cui non sia parte in giudizio, il Garante possa presentare osservazioni, da rendere per iscritto o in udienza, sulla controversia in corso con riferimento ai profili relativi alla protezione dei dati personali. Dunque, il Garante può intervenire nei procedimenti nazionali anche in veste di *amicus curiae*.

Spostando l'attenzione dal piano procedurale a quello sostanziale, pare opportuno richiamare un altro profilo: quello dei trattamenti dei dati nell'ambito del rapporto di lavoro.

L'art. 88 del Regolamento prevede che «gli Stati membri possano introdurre, con legge o tramite contratti collettivi (anche aziendali, ai sensi del *considerando* 155), norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro».

Il paragrafo 2 prevede che «[t]ali norme includono misure appropriate e specifiche a salvaguardia della dignità umana in particolare per quanto riguarda i sistemi di monitoraggio sul posto di lavoro ».

Ricordo che in questo contesto si inseriscono varie pronunce della Corte EDU. Fra queste la sentenza *Bărbulescu c. Romania*, in tema di controllo della corrispondenza elettronica (5 settembre 2017, Grande Camera) con cui viene ribaltata una pronuncia della sez. IV, 12 gennaio 2016, n. 61496/08, oggetto di varie critiche. Sulla scia della decisione *Bărbulescu* si pongono le sentenze *Antovič e Mirkovič c. Montenegro* del 28 novembre 2017 e *Ribalda e altri c. Spagna* dell'8 gennaio 2018, entrambe in tema di videosorveglianza[39].

La Corte EDU ha chiarito che l'art. 8 della CEDU, pur essendo essenzialmente rivolto a proteggere gli individui contro le interferenze arbitrarie delle autorità pubbliche, non stabilisce in capo allo Stato solo un'obbligazione negativa, ma anche un'obbligazione positiva che consiste nell'adozione di una normativa adeguata a tutela della *privacy* affinché le pur ammissibili ingerenze nella sfera privata del singolo siano controbilanciate da una serie di garanzie[40] anche di natura giurisdizionale.

Ai giudici nazionali spetta il compito di operare un non semplice bilanciamento tra il diritto dei lavoratori alla tutela della *privacy* del lavoratore e il diritto del datore ad effettuare controlli che possano garantire una efficace ed efficiente gestione delle attività aziendali. In questo esercizio, i giudici nazionali sono chiamati a dare alle norme interne una lettura convenzionalmente orientata, ma, ancor prima, conforme al nuovo Regolamento letto alla luce degli articoli 7 e 8 della Carta dei diritti fondamentali, disapplicando tali norme ove le antinomie rilevate non possano essere ridotte ricorrendo al criterio ermeneutico.

Il terzo paragrafo impone agli Stati membri di notificare alla Commissione le disposizioni di legge, adottate ai sensi del paragrafo 1, entro il 25 maggio 2018 e di comunicare senza ritardo ogni successiva modifica.

È rimesso, dunque, interamente agli Stati membri il compito di introdurre nei propri ordinamenti le garanzie necessarie a tutelare i lavoratori.

Nella sua proposta, la Commissione, al contrario, attribuiva a sé questo compito, da svolgere mediante l'adozione di atti delegati. Ancora diversa era la

---

[39] Cfr., per un commento alle sentenze della Corte EDU, G. FORMICI, *Lavoratori e tutela della* privacy*: l'evoluzione della giurisprudenza della Corte europea dei diritti dell'uomo, tra controllo della corrispondenza elettronica e videosorveglianza*, in www.osservatorioaic.it, 13.4.2018.

[40] Secondo la Corte EDU, nella sentenza *Bărbulescu*, i giudici per determinare la legittimità della misura di controllo attuata dal datore di lavoro devono valutare se: (*i*) il dipendente sia stato preventivamente informato del possibile svolgimento di controlli; (*ii*) il datore abbia dato chiare informazioni sull'entità, sul livello di ingerenza e intrusione, sulla durata e sull'estensione del controllo, nonché sul numero di soggetti che possono avere accesso agli esiti dei controlli; (*iii*) se le ragioni addotte dal datore per motivare le attività di controllo siano legittime; (*iv*) se non vi siano altre misure a disposizione del datore di lavoro, meno invasive di quelle adottate; (*v*) quali siano le conseguenze del monitoraggio; (*vi*) se siano previste misure di salvaguardia adeguate per il dipendente. Cfr. *ibidem*, p. 9.

Posizione comune del Parlamento europeo in prima lettura[41] che, invece, proponeva, con l'emendamento 192, di disciplinare in modo assai ampio e articolato le modalità e i limiti di intervento degli Stati membri, chiamati a completare le tutele per lavoratori. Sul punto si può menzionare anche il parere, relatrice Nadja Hirsch, della Commissione per l'occupazione e gli affari sociali del Parlamento europeo secondo cui «[n]ella sua versione attuale, e in particolare per quanto concerne la protezione dei dati dei lavoratori, il presente regolamento può solo offrire una protezione minima»[42].

L'art. 88 del Regolamento è, dunque, frutto di un compromesso politico, raggiunto il 15 dicembre 2015, fra le posizioni assunte dai due co-legislatori e dalla Commissione e poi ratificato il successivo 17 dicembre dalla Commissione (LIBE) del Parlamento europeo.

L'art. 9, paragrafo 2, lett. b) del Regolamento, infine, acconsente al trattamento dei dati sensibili anche in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui questo sia autorizzato da una norma dell'Unione o nazionale o anche da un contratto collettivo ai sensi del diritto degli Stati membri e purché si sia in presenza di garanzie appropriate per l'interessato.

Sembra emergere un afflato armonizzatore del Regolamento che al contempo riempie il silenzio della direttiva 95/46/CE. Il margine di manovra degli Stati membri è alquanto ampio, ma le direttrici sono state tracciate.

Secondo lo schema di decreto legislativo spetta sempre al Garante il compito di promuovere l'adozione di regole deontologiche che dovranno essere rispettate da soggetti sia pubblici sia privati, prevedendo anche specifiche modalità per le informazioni da rendere all'interessato (nuovo art. 111 del d.Lgs 196/2003).

Infine, lo schema di decreto opera un rinvio a quanto disposto dagli articoli 4, 8 e 38 dello Statuto dei lavoratori, che continua, dunque, a rivestire un ruolo centrale per la materia, sia dall'articolo 10 del d.lgs 10 settembre 2003, n. 276, che ha esteso il divieto di indagini sulle opinioni anche alle agenzie di lavoro e agli altri soggetti pubblici e privati autorizzati o accreditati.

Non resta, dunque, che attendere la versione definitiva del decreto legislativo per opportune considerazioni.

---

[41] Risoluzione legislativa del Parlamento europeo del 12.3.2014 sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Procedura legislativa ordinaria: prima lettura).

[42] Si legge nel Parere: «È opportuno che ciascuno Stato membro possa continuare a fissare norme più favorevoli per i lavoratori. Inoltre, deve essere possibile definire tali norme tramite accordi collettivi. La formulazione "nei limiti del presente regolamento" va respinta per diversi motivi. Innanzitutto, è in contraddizione con la deroga settoriale generale dell'articolo 82 e, in combinazione con gli atti delegati proposti dalla Commissione all'articolo 82, potrebbe portare a una situazione estremamente confusa. In secondo luogo, nell'ipotesi peggiore ciò potrebbe implicare che gli Stati membri non adottino regole più specifiche. Infine, la formulazione in questione sembra essere stata selezionata in modo arbitrario, dal momento che nel caso di altre clausole di apertura, ad esempio nel settore dei mezzi di comunicazione, tale limitazione non è presente».

4. L'ambito di applicazione territoriale del Regolamento (UE) 2016/679

L'art. 3, par. 1, prevede che «il […] 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». Si tratta di un aspetto innovativo rispetto alla direttiva 95/46/CE, essendo una caratteristica che riflette lo sviluppo della tecnologia moderna e di *Internet* e la necessità di tutelare i dati personali di soggetti residenti nel territorio dell'Unione anche nel caso in cui il loro trattamento sia effettuato al di fuori di esso.

Sebbene questo sia un profilo non disciplinato espressamente dalla direttiva, esso non rappresenta, nella sostanza, una vera e propria novità in quanto la giurisprudenza della Corte di giustizia aveva già chiarito la misura in cui la protezione dei dati personali doveva essere estesa anche in presenza di trattamenti dei dati effettuati al di fuori del territorio dell'Unione. Nella pronuncia *Google Spain*[43] la Corte aveva, infatti, dato un'interpretazione estensiva alla nozione di stabilimento di cui all'art. 4 della direttiva 95/46/CE[44]. Questi profili, ancorché sotto un'angolazione diversa inerente al potere dell'autorità di controllo nazionale di verificare che il trattamento e/o il trasferimento verso Paesi terzi di dati personali di un individuo che abbia proposto alla medesima autorità una domanda relativa alla protezione dei propri diritti e libertà personali, saranno poi ampiamente ripresi nella sentenza *Schrems* [45].

Il Regolamento opera, inoltre, un'ulteriore estensione della tutela in quanto nell'ambito di applicazione territoriale vengono fatti rientrare anche quei trattamenti di dati di soggetti che si trovano nel territorio dell'Unione, effettuati da un titolare o da un responsabile del trattamento che non siano stabiliti al suo interno, quando le attività di trattamento riguardino l'offerta di beni, la prestazione di servizi o il loro monitoraggio che abbia luogo sul territorio dell'Unione (art. 3, par. 2)[46].

5. Il principio di responsabilizzazione del titolare del trattamento dei dati personali quale principale novità del nuovo Regolamento

Il catalogo dei principi generali del trattamento dei dati personali è rimasto pressoché inalterato rispetto a quanto previsto dalla direttiva 95/46/CE. Si prevede sempre che il trattamento dei dati debba avvenire in modo lecito, corretto e trasparente nei confronti dell'interessato; che vi sia una limitazione della finalità

[43] Corte giust., sentenza *Google Spain*, cit.

[44] *Ibidem*, pt. 54 e 55.

[45] Corte giust., sentenza *Schrems*, cit. pt. 53, 57 e 63.

[46] Da ultimo, l'art. 3, par. 3, prevede l'efficacia del Regolamento rispetto al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

del trattamento; una minimizzazione del trattamento dei dati che devono essere adeguati, pertinenti e limitati alle finalità per le quali sono trattati; tali dati devono essere esatti e, se del caso, aggiornati; devono essere poi conservati per un periodo limitato e deve esserne garantita l'integrità e la riservatezza.

Piuttosto, ed è questa una delle principali novità introdotte dal Regolamento, è previsto che il rispetto di tali principi debba essere direttamente assicurato dal titolare del trattamento che viene, dunque, responsabilizzato. Il profilo da ultimo richiamato, anche noto con il termine anglosassone di *accountability*, è centrale nella nuova disciplina. Gli artt. 23-25, in particolare, e l'intero Capo IV del Regolamento, affidano ai titolari del trattamento il compito di deciderne autonomamente le modalità, le garanzie e i limiti applicativi nel rispetto dei principi generali.

L'art. 25 introduce un nuovo criterio, la c.d. "*data protection by default and by design*" (fin dalla progettazione e per impostazione predefinita), in virtù della quale occorre, prima ancora del trattamento dei dati, prevedere fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del Regolamento.

Spetta poi al titolare del trattamento effettuare una valutazione d'impatto iniziale, in particolare se è previsto l'uso di nuove tecnologie. Il titolare del trattamento in presenza di un rischio dovrà, in primo luogo, adottare tutte le misure necessarie per, possibilmente, escluderlo o mitigarne gli effetti. Dopodiché, egli potrà decidere in autonomia se iniziare il trattamento oppure consultare l'Autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale. Qualora, poi, la valutazione d'impatto indichi l'esistenza di un rischio elevato, la consultazione dell'Autorità di controllo è obbligatoria. Non spetta, dunque, all'Autorità di controllo il compito di "autorizzare" in via preventiva il trattamento, bensì quello di indicare al titolare le misure ulteriori (eventualmente) da adottare e, se necessario, quello di adottare tutte le misure correttive richiamate all'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

Questo processo di responsabilizzazione, avviato dal legislatore dell'Unione anche in altri settori, come quello della concorrenza, produrrà l'effetto di rendere l'intervento delle Autorità di controllo essenzialmente eventuale e successivo e, di conseguenza, farà venire meno l'obbligo, previsto dalla direttiva 95/46/CE, per il titolare di notifica preventiva dei trattamenti a tali autorità. Questo obbligo, per taluni soggetti e per taluni dati, è sostituito da quello di tenere un registro dei trattamenti[47].

Inoltre, va ricordato che il Regolamento introduce un meccanismo di "sportello unico" secondo cui, in casi aventi una significativa dimensione transfrontaliera, a prendere la decisione sarà l'autorità di controllo dello stabilimento principale o

[47] V. art. 30 del Regolamento in tema di registro delle attività di trattamento e, in particolare, il par. 5 del medesimo articolo ove si specifica che gli obblighi inerenti la tenuta di tali registri «non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10».

dello stabilimento unico del titolare, detta capofila, in quanto essa si trova in una posizione "più idonea" rispetto alle altre ventisette autorità nazionali a trattare il caso.

Il meccanismo, che prevede complesse modalità di coordinamento e cooperazione fra le varie autorità di controllo, non opera quando il trattamento è effettuato da autorità pubbliche o da organismi privati che agiscono nell'interesse pubblico. In tali casi l'unica autorità di controllo competente sarà quella dello Stato membro in cui l'autorità pubblica o l'organismo privato siano stabiliti.

6. Diritti nuovi e diritti "rafforzati" per l'interessato

A fronte del permanere del medesimo impianto di principi generali previsto dalla direttiva 95/46/CE, nuovi sono invece taluni diritti garantiti all'interessato che trovano il proprio fondamento nei principi generali stessi, mentre altri diritti vengono dal Regolamento solo rafforzati.

Non rappresenta una novità assoluta il c.d. "diritto all'oblio" che appartiene al nucleo originario di garanzie previste dalla Convenzione 108/1981 e, in virtù della giurisprudenza additiva della Corte di giustizia, anche dalla direttiva 95/46/CE, all'art. 12, lett. b) e dunque, a livello nazionale, dal Codice *Privacy* all'art. 7, comma 3, lett. b[48].

In particolare, la Corte, nella già richiamata sentenza *Google Spain*, ha ritenuto che sia necessario attraverso una valutazione caso per caso, operare un bilanciamento tra il diritto e l'interesse comune alla conoscenza di un determinato dato e il diritto del soggetto interessato a ottenerne la cancellazione[49]. Il diritto all'oblio, altrimenti definibile come il diritto a una cancellazione rafforzata, con tale precisa ed evocativa denominazione e con contorni applicativi più estesi rispetto a quanto previsto dal *Codice Privacy*, è oggi disciplinato dall'art. 17 del Regolamento. Tale norma, la cui formulazione diverge da quella contenuta nella proposta della Commissione, prevede un elenco dei casi in cui l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, ossia: «*a*) quando i dati personali raccolti o trattati non risultano più necessari rispetto alle finalità del trattamento; *b*) quando l'interessato abbia revocato il consenso e non sussista altro fondamento giuridico per il trattamento; *c*) quando l'interessato si opponga al trattamento e non sussista alcun motivo legittimo prevalente per procedere al trattamento; *d*) quando i dati personali siano stati trattati illecitamente; *e*) quando i dati personali debbano essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; *f*) quando i dati personali

[48] V. L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 262 ss.

[49] Corte giust., sentenza *Manni*, cit., nonché sentenza *Google Spain*, cit.

siano stati raccolti relativamente all'offerta di servizi della società dell'informazione»[50].

Il diritto alla cancellazione dei dati, invece, non sussiste «nella misura in cui il relativo trattamento sia necessario: *a*) per l'esercizio del diritto alla libertà di espressione e di informazione; *b*) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; *c*) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3; *d*) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o *e*) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria»[51].

Tra i diritti di effettiva nuova introduzione, figura quello alla portabilità dei dati personali, di cui all'art. 20 del Regolamento, ovvero 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» nonché il diritto, dello stesso interessato, di «trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti». Tale diritto sorge solo nel caso di un trattamento effettuato con mezzi automatizzati e presuppone il consenso o la presenza di un contratto stipulato con l'interessato.

7. Alcune considerazioni conclusive

Il Regolamento (UE) 2016/679 non può certamente rappresentare un approdo definitivo della materia, e ciò non solo perché la disciplina dovrà essere necessariamente completata da atti delegati che la Commissione è chiamata ad adottare ai sensi dell'art. 92 e da atti di esecuzione sia a livello di Unione europea, sia a livello nazionale che dovranno occuparsi della materia in una chiave dinamica e non statica, ma anche perché questa normativa, che pure si apprezza per alcuni profili, lascia aperti numerosi dubbi interpretativi che, è facile preconizzare, saranno rivolti alla Corte nell'ambito delle sue competenze pregiudiziali previste dall'art. 267 del TFUE.

In aggiunta (e questa è la nota più dolente) si pongono non pochi problemi di coordinamento tra questa normativa e quella degli Stati membri. Problemi, paradossalmente, acuiti dalla natura dell'atto che sì ha la forma di un regolamento, ma che al tempo stesso contiene una disciplina incompleta e, talora, forse volutamente vaga.

[50] Cfr. art. 17, par. 1 del Regolamento generale.
[51] Cfr. art. 17, par. 3 del Regolamento generale.

Un ruolo importante sarà sempre svolto dal Gruppo di lavoro che, costituito in attuazione dell'art. 29 della direttiva 95/46/CE, a partire dalla data di applicazione del Regolamento 2016/679/CE, assumerà la denominazione di Comitato europeo per la protezione dei dati con il compito di «creare una cultura di protezione dei dati comune fra tutte le autorità nazionali di controllo allo scopo di garantire l'interpretazione coerente delle disposizioni del regolamento»[52]. Il Gruppo di lavoro, composto dalle autorità nazionali garanti della protezione dei dati e dal Garante europeo dei dati personali, ha, peraltro, già svolto un ruolo importante nel definire talune problematiche inerenti alla corretta applicazione del Regolamento, avendo adottato a partire dalla sua entrata in vigore una serie di pareri, prese di posizioni e linee guida. Fra le principali linee guida adottate dal Gruppo di lavoro "Articolo 29" vi sono quelle in tema di consenso al trattamento dei dati[53], in materia di *data protection risk assesment*[54], sulla profilazione dei dati[55], sulla trasparenza[56] nonché sulla portabilità dei dati[57].

Di sicuro, non mancheranno ulteriori interventi chiarificatori. Nonostante le buone intenzioni, e pur rimanendo valido in termini di obiettivi e principi, il quadro giuridico che si viene a comporre con l'applicazione del Regolamento, appare, infatti, nel suo complesso alquanto frammentato e non idoneo a introdurre sufficienti elementi di solida certezza giuridica.

---

[52] V. art. 68 del Regolamento generale. V., anche, COM(2018) 43 def, cit., spec. p. 10 secondo cui «il Comitato europeo per la protezione dei dati sarà un organismo dell'Unione dotato di personalità giuridica incaricato di garantire l'applicazione coerente del regolamento. Sarà composto dalla figura di vertice di ciascuna autorità di protezione dei dati e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti».

[53] Article 29 Working Party, *Guidelines on consent under Regulation 2016/679*, del 28.11.2017 del 10.4.2018, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

[54] Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, del 4.10.2017, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[55] Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, del 6.2.2018, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

[56] Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, dell'11.4.2018, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

[57] Article 29 Working Party, *Guidelines on the right to data portability,* del 5.4.2017, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.