UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Sede Amministrativa: Università degli Studi di Padova

Dipartimento di
DIRITTO PUBBLICO COMPARATO, INTERNAZIONALE E COMUNITARIO (DiPIC)

CORSO DI DOTTORATO DI RICERCA IN GIURISPRUDENZA
CURRICOLO IN DIRITTO COSTITUZIONALE (Area Pubblicistica)
CICLO 32°

# DIRITTI FONDAMENTALI E *BIG DATA*

# I PROFILI COSTITUZIONALI DELLA PROTEZIONE DEI DATI PERSONALI TRA DIRITTO ITALIANO E EUROPEO

**Coordinatore:** Ch.mo Prof. Roberto E. Kostoris
**Supervisore**: Ch.mo Prof. Mario Bertolissi

**Dottorand**o : dott.ssa Elisa Spiller

# Diritti fondamentali e big data

*I profili costituzionali della protezione dei dati personali tra diritto italiano e europeo*


*– ABSTRACT –*

La tesi si propone di affrontare le questioni legate all'impatto dei *big data* sui diritti fondamentali, concentrando l'attenzione sulla funzione costituzionale del diritto alla protezione dei dati personali nel contesto italiano ed europeo.
Dopo aver dato conto del percorso svolto dal diritto internazionale ed europeo per definire i fondamenti di tale disciplina e le implicazioni costituzionali delle garanzie che propone, viene esaminato con particolare attenzione il quadro normativo interno, analizzando come il Giudice delle leggi e il legislatore nel tempo abbiano affrontato il rapporto tra diritti e informazioni. Specifica attenzione è rivolta soprattutto all'individuazione dei molteplici interessi intercettati da questa disciplina e ai criteri di bilanciamento da essa indicati per procedere alla ricomposizione dei conflitti tra prerogative confliggenti.
L'analisi si sofferma inoltre sul sistema di tutele elaborato a livello comunitario, concentrandosi inizialmente sul primo c.d. *data protection package*, per poi passare a considerare la nuova strategia di *data-governance* europea e i contenuti del reg. 679/2016. Facendo ciò, si approfondiscono in particolare il percorso che ha portato il legislatore europeo a riconoscere la protezione dei dati personali come diritto fondamentale dell'UE (art. 8 CDFUE) e le implicazioni che questo ha avuto sul piano delle competenze comunitarie (art. 16 TFUE).
Da ultimo, alla luce delle considerazioni appena accennate, viene proposto un *case-study* in cui si affrontano i problemi che vengono emergendo da questa progressiva comunitarizzazione della disciplina sulla protezione dei dati personali, soprattutto nei rapporti tra la Corte di giustizia UE e i giudici costituzionali nazionali. Chiude il lavoro una riflessione circa le prospettive che si aprono per il c.d. costituzionalismo tecnologico europeo a il ruolo che spetta all'Unione e agli Stati membri nel promuovere questa trasposizione delle tradizionali garanzie a favore dei diritti fondamentali.

* * *

The dissertation aims to tackle the issues emerging by the use of big data analytics on fundamental rights. The attention focuses on the constitutional analysis of the fundamental right to the protection of personal data, and the goal is to compare the different approaches developed by EU law and national law on this topic.

The first part gives a short introduction to the overall outline of the study, defining the structure and the methodology. After that, the second part provides a brief overview of the gist of the international and European data protection strategies, then it analyses on the national legal framework. In particular, the core of this chapter focuses on the approach developed by the Italian Constitutional Court about the issues concerning privacy and data protection. Furthermore, it pays precise attention to the many interests intertwined by personal data analytics and to the standards developed by the domestic constitutional case-law to balance the opposite prerogatives involved these processings.
In light of the recent Italian case-law on the relation between the national and the European legal systems, the third part develops the evolution of the EU discipline on data protection. As first, it focuses on the first data protection package launched in the 90s. It then addresses the issues concerning the ongoing debate on the current EU strategies on data-governance, highlighting on the novelties introduced by the regulation 2016/679/EU. So doing, the study devotes particular attention the constitutionalization process of data protection in the supranational legal system. In particular, it focuses on article 8 of the Charter of Nice and article 16 TFEU.
Finally, the last part provides a case study focused on the EUCJ case-law on data and fundamental rights. This section aims to address the issues emerging in this progressive shift of the constitutional guarantees on data protection towards the Luxemburg Court. In particular, the research focuses on the institutional dialogue developed between the EUCJ and the national constitutional courts on these themes. The work concludes providing some provisional disclosures on this complicate evolution of the EU technological constitutionalism, remarking on the contact points that animate this multilevel system of protection.

## INDICE

# Capitolo 1

## Diritti e dati: una breve introduzione
## *I profili costituzionali della protezione dei dati personali tra diritto italiano e europeo al tempo dei big data*

### 1. Premessa

L'obiettivo di questo lavoro di ricerca è quello di indagare il rapporto che oggi intercorre tra diritto nazionale e diritto europeo nell'elaborazione delle strategie di *data governance*, soprattutto per quanto riguarda la definizione del quadro normativo necessario alla tutela dei diritti fondamentali.

Soprattutto dopo l'entrata in vigore del reg. 679/2016, il tema ha attirato particolare attenzione in diversi settori: dal diritto pubblico europeo, al diritto internazionale, finanche nell'ambito degli studi di diritto costituzionale. È ormai chiaro come dal corretto utilizzo dei dati personali dipendano infatti una pluralità di interessi; non ultimi alcuni diritti fondamentali condivisi dalla tradizione costituzionale europea, dal diritto alla riservatezza, alla sicurezza, alla proprietà intellettuale, alla libertà di espressione.

Ciò non di meno, si avverte che con l'avvento del fenomeno dei c.d. *big data* i problemi che oggi si cominciano ad affrontare in questo campo, nel corso degli anni a venire saranno destinati ad assumere proporzioni ben più estese. Sono infatti molteplici gli ambiti in cui attività e procedimenti prima svolti in modalità analogica vengono oggi sostituiti da nuove applicazioni digitali, così automatizzando una pluralità di processi operativi e decisionali.

Lo scopo di queste prime pagine, dunque, è quello di porre le debite premesse, individuando innanzitutto il rapporto tra diritto costituzionale e nuove tecnologie, per poi delineare, nello specifico, le questioni che legate all'impatto dei dati sui diritti fondamentali.

### *1.1. Nuove tecnologie, nuovi diritti*

Il punto di partenza da cui poi si snoda il filo conduttore di questa ricerca consiste nel rapporto tra *tecnologia* e *diritto*. Come ci sarà modo di vedere a breve, non si tratta di un tema estraneo agli studi di diritto costituzionale. Tuttavia, è un argomento che, in ambito giuridico, trova uno sviluppo trasversale, intercettando ambiti ben diversi.

Questo è dovuto essenzialmente al fatto che nel settore tecnologico, forse più che ogni altro, gli elementi *meta*-giuridici – i *fatti*, prima ancora delle *fattispecie* – giocano un ruolo essenziale nel plasmare la realtà circostante, intercettando e plasmando la realtà circostante in modo assolutamente inedito. Applicazioni pensate o inventante (nel senso letterale del termine, come *invenute* e cioè *trovate*) per un singolo settore – medico, industriale, militare – possono segnare il passaggio di un epoca, trasfigurando i tratti che avevano caratterizzato la vita dei singoli e l'organizzazione sociale fino a quel momento.

I molteplici impatti delle diverse rivoluzioni, in alcuni casi, sono stati assimilati nel tempo, elaborando nuove coordinate concettuali e valoriali per ricollocare la persona umana in queste nuove rappresentazioni della realtà fisica e sociale[1]. Ciò non di meno, il giurista, di fronte a questi nuovi scenari, il più delle volte si trova di fronte a qualcosa si assolutamente inedito. Così come da un punto di vista

[1] J.C. DE MARTIN, *Introduzione,* a L. FLORIDI, *La rivoluzione dell'informazione* (titolo originale: *Information – A very short introduction*), Torino, Codice Edizioni, 2012.

scientifico e filosofico, i periodi di cambiamento rappresentano, infatti, un'occasione per rimeditare le precedenti convinzioni, nel mondo del diritto si rende necessario testare nuovamente la portata delle categorie e delle figure a disposizione: il concetto di persona, l'idea di libertà, l'equilibrio tra interessi collettivi e individuali e via dicendo. Più le rivoluzioni risultano immanenti alla vita delle persone – e in grado di incidere nelle dinamiche sociali – più i giuristi a partire dai *fatti* dovranno verificare se e come l'«armamentario di formine»[2] ereditate dalla tradizione trovi ancora una qualche corrispondenza nei nuovi contesti che si vengono a delineare.

Di fronte alle rivoluzioni del Novecento, quest'esigenza è emersa in modo quanto mai evidente. Guardando alle preoccupazioni legate allo sviluppo delle tecnologie dell'informazione, al surriscaldamento globale, all'inquinamento e alla tutela dell'ambiente, il legislatore – a livello nazionale e non solo – avverte di trovarsi ad affrontare problemi assolutamente inediti[3]. La logica e le categorie tradizionali, in questi frangenti, richiedono un profondo rinnovamento, verso una rilettura del quadro normativo tagliata sulle esigenze della contemporaneità.

È in questi frangenti che, per assicurare uno sviluppo economico e tecnologico allineato con i valori e l'identità della società che li accoglie si sviluppa la dialettica dei c.d. «*nuovi diritti*». Di fronte a tecnologie nuove si avverte l'esigenza di riaffermare una serie di pretese volte a far valere anche in questi contesti i principi e le prerogative ereditati dalla tradizione costituzionale e dei diritti umani, in un confronto tra giudici e corti teso a riconfermare a livello nazionale e sovrannazionale i principi dello Stato di diritto.

---

[2] Così, efficacemente, in G. ZAGREBELSKY, *Il diritto mite*, Torino, Einaudi, 1992, p. 217.

[3] F. HONDIUS, *Emerging Data Protection in Europe*, Amsterdam, North-Holland Publishing Company, 1975, pp. 2 ss.

*1.2 Le sfide del costituzionalismo "tecnologico"*

Nell'esperienza del diritto positivo, depositarie di questa tradizioni dei diritti e del diritto sono storicamente le Carte costituzionali. È per questo che, di prassi, il tema dei c.d. «nuovi diritti» trova ampio spazio nel dibattito costituzionale[4]. La funzione delle Corti, chiamate a giudicare della conformità delle evoluzioni ordinamenti con i principi stabiliti dalle Leggi fondamentali, è legata proprio alla volontà di garantire vitalità all'ordinamento.

Come ricorda Stefano Rodotà

> Un'interpretazione restrittiva del ruolo delle corti costituzionali, la fine del loro "attivismo", possono diventare il modo per inceppare il più forte motore di una dinamica che vede il riconoscimento dei diritti fondamentali non come una vicenda esaurita una volta per tutte, nel giorno lontanissimo dell'approvazione di un testo costituzionale, ma come un compito mai concluso, che richiede un confronto continuo tra principi di base ed esigenze che la realtà sempre mutevole viene proponendo[5]

Gli sviluppi della giurisprudenza italiana – e non solo – confermano appieno questa considerazione. Lo sviluppo di nuovi mezzi di comunicazione, le conquiste scientifiche (soprattutto in ambito medico), l'affermarsi di una consapevolezza sociale rispetto ai temi legati all'innovazione. Dal diritto all'informazione [6] al pluralismo informativo[7], dall'interruzione volontaria di gravidanza[8] al c.d. «diritto a procreare»[9], dalla tutela dell'ambiente[10] alla sicurezza degli organismi geneticamente

---

[4] F. MODUGNO, *I nuovi diritti nella giurisprudenza costituzionale*, Torino, Giappichelli, 1995; S. MORELLI, *Tecniche di tutela dei diritti fondamentali della persona: nuovi diritti nella giurisprudenza della Corte costituzionale, di Cassazione, europea di Strasburgo, tutela preventiva e risarcitoria*, Padova, Cedam, 2003; A. D'ALOIA (a cura di), *Biotecnologie e valori costituzionali*, Torino, Giappichelli, 2005.

[5] S. RODOTÀ, *Repertorio di fine secolo,* Roma, Laterza, 1999, p. 27.

[6] Corte cost., sent. n. 112 del 1993 e, in precedenza sentt. nn. 122 del 1970; 105 del 1972; 1 del 1981 e 194 del 1987.

[7] Corte cost. sent. n. 225 del 1977 e, in seguito sent. n. 155 del 2002.

[8] Corte cost. sent. n. 27 del 1975.

[9] Corte cost. sent. n. 347 del 1998 e, in seguito ord. n. 369 del 2006, sentt. nn. 151 del 2009; 162 del 2014, 96 del 2015; 229 del 2015; 84 del 2016; 272 del 2017.

modificati[11]; una serie di conquiste ormai acquisite, sono il frutto di una lettura aperta e dinamica del dettato costituzionale, ancor oggi fonte di risposta alle molteplici istanze di tutela che si sollevano dalla vita della cittadinanza e dell'attività giudiziaria.

Rispetto alle tecnologie dell'informazione e soprattutto alla diffusione della rete, l'«attivismo» del Giudice delle leggi, sul fronte interno, sembra però essere più tiepido rispetto ad altri temi (se non quasi assente). Se in un primo momento, negli anni Settanta, le sentenze sul diritto alla riservatezza avevano contribuito ad assicurare copertura costituzionale ad un diritto che fino ad allora era rimasto nel limbo, in seguito, con lo sviluppo delle tecnologie dei dati e l'avvento dell'I*nternet*, fatte salve poche eccezioni, il processo di riconoscimento di «nuovi diritti» costituzionali in campo tecnologico si è in qualche modo intiepidito.

Certamente – come osservato – un simile ripiegamento potrebbe essere giustificato da un generale ridimensionamento delle decisioni in tema di diritti[12] (e così anche dei nuovi diritti legati alla dimensione tecnologica). Tuttavia, non sembra infondato il monito che proviene da chi rimane perplesso rispetto a quest'atteggiamento[13], soprattutto considerando le forti implicazioni etiche e sociali legate alla tutela dei diritti fondamentali in una società sempre più liquida, globalizzata, digitale – ed ora – algoritmica[14].

---

[10] *Ex multis,* Corte cost. sent. nn. 151 del 1986, 210 del 1987 617 del 1987; 641 del 1987; 1031 del 1988.

[11] Corte cost. sent. n. n. 150 del 2005, 116 del 2006.

[12] P.A. CAPOTOSTI, *La Corte costituzionale: giudice delle libertà o dei conflitti?*, in B. CARAVITA (a cura di), *La giustizia costituzionale in trasformazione: la Corte costituzionale tra giudice dei diritti e giudice dei conflitti*, Jovene, Napoli, 2012, pp. 277 ss.

[13] P. PASSAGLIA, *Corte costituzionale e diritto dell'Internet: un rapporto difficile (e un appuntamento da non mancare)*, in *Giur. Cost.* 2014, n. 6; P. COSTANZO, *I diritti nelle "maglie" della Rete*, in L. BRUSCAGLIA, R. ROMBOLI, *Diritto pubblico e diritto privato nella rete delle nuove tecnologie*, Pisa, 2010, 5 ss.

[14] Non mancano riferimenti in merito anche nelle edizioni più recenti di diffusi manuali istituzionali, come documentano gli aggiornamenti in R. BIN, G. PITRUZZELLA, *Diritto Pubblico*, Torino, Giappichelli, 2017, pp. 477 ss. (in cui gli Autori dedicano qualche pagina a «*la sfida di internet e dei social*» e «*il ruolo dei* gatekeepers», interrogandosi sulla possibilità di diventare «*schiavi di un algoritmo?*») o ancora in

Di fronte ad uno scenario simile, oltre alle questioni relative alla tutela dei diritti fondamentali, emergono nuovi problemi legati alla progressiva tecnologizzazione dell'agire pubblico e al manifestarsi di nuovi poteri – economici e sociali – in capo ai grandi giganti tecnologici come Apple, Amazon, Alphabet (Google), Microsoft, Facebook (le c.d. *big tech giants*). Oltre alle interferenze con il diritto alla riservatezza, si avverte come con il progressivo affermarsi di questo nuovo paradigma di efficienza, fondato sul potenziale dei dati e degli algoritmi, possa essere inficiata la tenuta di alcune garanzie fondamentali, come i principi di tutela contro le diseguaglianze, il giusto processo, la partecipazione e al controllo pubblico rispetto all'agire pubblico e, più in generale, la trasparenza di tutti quei procedimenti decisionali che a diverso titolo, per mano di attori pubblici o privati, possono produrre effetti significativi sulla sfera giuridica dei soggetti interessati e nel godimento dei loro diritti fondamentali.

Come osservato, dunque, se, oltre il momento costituente vero e proprio, il costituzionalismo in sé può essere letto come la continua ridefinizione dei limiti rivolti poteri pubblici, al fine di preservare la dignità e la libertà dei singoli nel loro determinarsi rispetto a sé e al contesto nei diversi contesti[15], si cominciano ad intuire quali sfide si prospettino per il c.d. costituzionalismo "tecnologico". Si rende infatti necessaria una rilettura dei valori della Carta, nell'ottica di promuovere una «Costituzione continuamente attualizzata»[16].

È opportuno parlare di valori, prima ancora che di diritti, poiché di fronte alla continua stratificazione delle fonti – nazionali e sovrannazionali – che oggi

---

[15] Così intendendo non solo quelli riconducibili agli attori pubblici in senso stretto, ma a tutti quelli che, in qualche modo, esercitano delle prerogative che incidono sulla dimensione pubblica, cioè sociale. Per alcuni interessanti approfondimenti sul rapporto tra diritto costituzionale e diritto privato rispetto al valore orizzontale dei diritti fondamentali si rimanda a H.W. MICKLITZ, *Introduzione*, in ID. (a cura di) *Constitutionalization of European Private Law*, Oxford, Oxford University Press, 2014, pp. 5 ss.

[16] G. TIEGHI, *Per una «Costituzione continuamente attualizzata»: Corte costituzionale e* overruling, in M. BERTOLISSI (a cura di), *Riforme. Opinioni a confronto*, Napoli, Jovene, 2015, p. 135.

concorrono a plasmare il c.d. costituzionalismo dei diritti[17] sarebbe fuorviante riferirsi immediatamente al contenuto precettivo del dettato costituzionale.

Di fronte questo scenario che si rinnova, infatti, rimangono saldi i punti di riferimento. Clausole essenziali come quelle contenute all'art. 2 Cost., con riferimento al «riconoscimento dei diritti inviolabili», o al successivo art. 3 Cost., circa la «pari dignità sociale» di tutti i cittadini, fungono da leva per creare nuovi spazi di confronto per la regolazione delle tecnologie informatiche. I principi che accomunano nei loro tratti essenziali la tradizione costituzionale di diversi Stati e che trovano da tempo spazio anche nelle principali Carte e Dichiarazioni internazionali, in questo momento rappresentano l'ancoraggio teorico e concettuale per pensare alle possibile evoluzioni della disciplina di questa materia, il "parametro" ultimo cui ancorare l'interpretazione delle norme di dettaglio e il comune punto di riflessione per tradurre sul piano del diritto le istanze etiche che accompagnano lo sviluppo delle tecnologie *data-intensive*.

## 2. Individuazione del problema

Entro le maglie della dottrina costituzionale, le conseguenze e le implicazioni della digitalizzazione sui diritti fondamentali sono un tema ormai studiato da molti anni e questa lunga riflessione, ai nostri fini, può fornire delle importati indicazioni di metodo. Prima con la diffusione dei computer e con la liberalizzazione dell'informatica, poi con l'avvento della rete e del *web*, la c.d. «rivoluzione

[17] G.F. FERRARI, *I diritti fondamentali dopo la Carta di Nizza. Il costituzionalismo dei diritti*, Milano, Giuffrè, 2001.

dell'informazione»[18], infatti, non smette di sollevare nuovi interrogativi, sfidando la tenuta delle garanzie tradizionali.

In risposta a questi fenomeni, sul piano del diritto costituzionale, nel tempo si sono fatte strada varie ipotesi, spaziando dalla possibilità di emendare la Carta in chiave tecnologica[19] all'idea di introdurre *ex novo* delle moderne dichiarazioni per la tutela dei diritti *online*[20].

Tuttavia, prima di intraprendere questi tentativi, è necessario comprendere e definire le caratteristiche e il contesto tecnologico che si intende analizzare. È cioè indispensabile capire che tipo di innovazione apporti ogni passo di questo sviluppo a quello precedente e così quali criticità possano rispetto al previgente quadro di riferimento. Solo così, infatti, si è in grado di cogliere come le tecnologie *data-intensive* possano costituire un fattore condizionante l'esercizio dei diritti fondamentali e così come l'ordinamento può reagire a fronte di queste situazioni.

### *2.1. Alcune definizioni necessarie: big data e intelligenza artificiale*

Per comprendere adeguatamente la portata del cambiamento in atto, è utile delineare l'oggetto materiale di questo studio, così da giustificare meglio, poi, le

---

[18] L. FLORIDI, *La rivoluzione dell'informazione,* Torino, Codice Editore, 2012, p. 10 ss. Argomento poi ripreso e ampliato in L. FLORIDI, *Quarta rivoluzione,* Milano, Raffaello Cortina Ed., 2016.

[19] Ben noti sono ormai gli ammonimenti in tal senso. In particolare, basti ricordare tra tutti gli ammonimenti promossi da Stefano Rodotà, il quale suggeriva che «in Italia una modifica dell'art. 21 della Costituzione potrebbe avere la forma seguente: "*Tutti hanno eguale diritto di accedere alla rete Internet, in condizioni di parità, con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale.*"» (in ID, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma, 2014, p. 16).

[20] E, in tal senso, spicca il tentativo promosso in Italia dalla Camera dei Deputati, in seno alla Commissione per i diritti e i doveri relativi ad Internet, le quali, il 14 luglio 2015, hanno approvato la *Dichiarazione dei diritti di Internet;* il primo *bill of rights* digitale elaborato in una sede istituzionale e approvato all'unanimità da un corpo parlamentare. A commento si rimanda, in particolare, a A. MASERA, G. SCORZA, *Internet, i nostri diritti*, Roma, Laterza, 2016.

preoccupazioni che esso solleva rispetto all'attuale stato dell'arte sul fronte normativo e giurisprudenziale.

Non servono particolari capacità d'analisi per rendersi conto di come l'ecosistema informativo in cui siamo immersi negli ultimi vent'anni sia profondamente cambiato. Con l'avvento e la diffusione del *web 2.0* e dei nuovi dispositivi *smart,* le interazioni economiche e sociali mediate dalla rete si sono moltiplicate in termini esponenziali. Ad una prima ricognizione, nel 2013, l'Organizzazione per la cooperazione e lo sviluppo economico (OECD) osservando lo scenario che allora si cominciava a prospettare sottolinea:

> The shift from analogue to digital technology has led to a much greater capacity to store and share pictures and video. Mobile devices enable the routine collection of geolocation information that locates individuals in time and space. Sensors used in health, environment and energy sectors produce data that can be linkable back to individuals. And much of this data is made available globally, supported by communications networks that permit continuous, multipoint data flows[21]

Considerazioni quanto mai vere. Ogni istante, infatti, la navigazione sul *web*, l'utilizzo dei *social network*, i vari sistemi di videoripresa presenti nei luoghi pubblici e privati, la geo-localizzazione, i sensori presenti nei dispositivi più diversi (dagli *smartphone* ai veicoli) producono un'esorbitate e continuo flusso di informazioni[22]: un vero e proprio «*tzunami informativo*»[23].

---

[21] OECD, *Exploring the economics of personal data: a Survey of Methodologies for Measuring Monetary Value*, del 2 aprile 2013, p. 7.

[22] Si tratta di una descrizione dal perimetro piuttosto variabile, proposta e ridefinita da diversi autori. Si vedano, *ex multis,* V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, Garzanti, 2013, *passim*; A. REZZANI, *Big Data: Architettura, tecnologie e metodi per l'utilizzo di grandi basi di dati*, Milano, Apogeo, p. 25 ss.; G. SHROFF, *The Intelligent Web. Search, Smart Algorithms, and Big data,* Oxford, Oxford University Press, 2015, p. xiii.

[23] In questi termini, D.E. HOLMES, *Big Data: A Very Short Introduction*, Oxford, Oxford University Press, 2017, p. 1 ss. Negli stessi termini, seppur con una metafora diversa, L. FLORIDI, *La rivoluzione dell'informazione*, cit., p. 7 (in cui si accenna, appunto ad un *exaflood*, «un neologismo coniato per qualificare questo tzunami di dati che sta sommergendo il mondo).

Non si tratta di un questione meramente tecnologica, bensì, come suggerito da Karen Yeung, di un *sociotechnical assemblage*. Qui si intrecciano lo sfruttamento dei dati e le logiche che guidano gli algoritmi, le caratteristiche dei dispositivi e l'*expertise* di quanti progettano questi sistemi, il potere di chi li distribuisce, la libertà di chi li usa, di chi – non ultimo – si trovano ad esserne oggetto[24].

Alla luce di questi elementi, soprattutto nel contesto europeo, la definizione di *big data* si è resa nel tempo sempre più inclusiva, sorpassando il tradizionale paradigma delle tre *v* (volume, velocità, varietà)[25] per accogliere una lettura più sistematica del fenomeno che accompagna queste tecnologie. Come sottolineato dal Garante europeo sulla protezione dei dati personali,

> «il termine megadati (big data) si riferisce alla crescita esponenziale sia della disponibilità sia dell'utilizzo automatizzato di informazioni, indicando enormi serie di dati digitali detenuti da società, governi e altre organizzazioni di grandi dimensioni, successivamente analizzati in modo estensivo (da cui il nome "analisi") attraverso algoritmi informatici»[26],

E si indentificano così tutte le pratiche con cui è possibile «combinare enormi volumi di informazioni di provenienza diversa e di analizzarli, spesso con l'ausilio di algoritmi di autoapprendimento per prendere decisioni informatizzate»[27].

Soprattutto quest'ultimo rilievo lascia intendere il grande potenziale di questi sistemi. I *big data*, infatti, non solo permettono di aggregare e riorganizzare contenuti provenienti da diverse fonti per offrire rappresentazioni inedite dello *status quo*.

---

[24] K. YEUNG, *Algorithmic Regulation: A Critical Interrogation*, in *Regulation & Governance*, 31 luglio 2017, p. 506.

[25] Paradigma elaborato all'inizio del nuovo millennio da Doug Laney, nel suo celeberrimo *3D Management: Controlling Data Volume, Velocity and Variety,* MetaGroup (Gartner Data & Analytics), File 949, 6 febbraio 2001. Questo modello, sebbene poco descrittivo nel merito, è oggi comunemente ripreso anche in ambito tecnico-giuridico. Cfr. *ex multis,* J. POTESTA, *Big Data: Seizing Opportunities, Preserving Values* ("Rapporto Potesta"), Ufficio esecutivo del presidente, Washington, maggio 2014, p. 2. G. D'ACQUISTO, M. NALDI, *Big data e Privacy by Design*, Torino, Giappichelli, 2017, p. 5.

[26] Gruppo di lavoro Articolo 29, *Parere 3/2013 sulla limitazione delle finalità*, del 2 aprile 2013, p. 35 ss.

[27] Garante europeo della protezione dei dati personali, *Verso una nuova etica digitale. Dati, dignità e tecnologia*, parere n. 4, 11 settembre 2015, p. 7.

Promettono soprattutto di fornire una prefigurazione degli ipotetici sviluppi di una certa situazione, delegando agli algoritmi non solo un'attività conoscitiva ma anche una responsabilità previsionale e decisionale rispetto ai compiti per cui sono impiegati. L'imperativo di fondo, dunque, è essenzialmente uno: «*lasciar parlare i dati*»[28].

Perché tutto ciò accada, tuttavia, è imprescindibile poter disporre di sistemi in grado di elaborare adeguatamente i diversi contenuti trasformando quelli che in origine sono soltanto dei sottoprodotti informativi (c.d. *raw data*, lett. "dati grezzi") in un insieme di contenuti coerenti e prontamente utilizzabili in diversi contesti (c.d. *smart data*, lett "dati intelligenti").

Per far questo, nel tempo, sono stati messi a punto *software* sempre più sofisticati e, proprio per la quantità di dati oggi a disposizione, l'ottimizzazione delle prestazioni e le capacità di estrazione e di analisi dei diversi *dataset* ha portata un crescente livello di automatizzazione delle procedure[29].

A riguardo, è utile quindi fare almeno un accenno al tema della c.d. intelligenza artificiale; un campo di studi che sta approfondendo in più direzioni il potenziale dei sistemi "intelligenti" intercettando sempre più spesso anche la ricerca in ambito giuridico[30].

---

[28] V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, Garzanti, 2013, p. 15.

[29] A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 1/2019, p. 92.

[30] F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, Giappichelli, 2018. Si tratta, in realtà, di un ambito particolarmente vasto, in cui rientrano sistemi e applicazioni di diverso tipo. Quel che qui interessa, ovviamente, non è tanto approfondire le caratteristiche di ognuna e, men che meno, le conseguenze che possono derivare da ciascuna di essere sul piano del diritto. L'intento è ben più modesto. Si tenterà soltanto di introdurre una prima definizione di quel che si intende per intelligenza artificiale in ambito politico-legislativo, per poi approfondire come queste tecnologie possono costituire un fattore condizionante nella realtà del diritto e – soprattutto – nell'esercizio dei diritti.

Se si cerca una definizione "minima"[31] di intelligenza artificiale (IA) quella oggi proposta a livello europeo è formulata in questi termini:

> *Intelligenza artificiale* (IA) indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi.
>
> I sistemi basati sull'IA possono consistere solo in software che agiscono nel mondo virtuale (ad esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale), oppure incorare l'IA in dispositivi di hardware (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'internet delle cose).[32]

Tuttavia, a motivo dei recenti progressi registrati in quest'ambito, sono già state messe in luce alcune peculiarità qui rimaste inespresse. I *software* di intelligenza artificiale, infatti, come accennato poc'anzi ragionando sui *big data*, dato un obiettivo complesso,

> agiscono nella dimensione fisica o digitale percependo il proprio ambiente attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulle conoscenze, o elaborando le informazioni derivate da questi dati e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo dato. I sistemi di IA possono usare regole simboliche o apprendere un modello numerico, e possono anche adattare il loro comportamento analizzando come l'ambiente è influenzato dalle loro azioni precedenti[33].

Simili considerazioni permettono di intuire facilmente come applicazioni dotate di un simile potenziale possano trovare spazio in ambiti ben diversi, ridefinendo le logiche operative ed epistemologiche dei contesti in cui si collocano. Le implicazioni sul piano del diritto, dunque, potrebbero essere molteplici, spaziando in settori assai diversi tra loro. Si rende quindi necessaria un'inevitabile circoscrizione del campo di indagine. Dopo alcune brevi premesse, dunque, nel

---

[31] Oltre ad ammettere altre precisazioni, gli esperito consultati in tal senso dalla Commissione europea precisano che la definizione può essere ampliata allo scopo di chiarire alcuni aspetti relativi all'IA come disciplina scientifica e come tecnologia. Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale istituto dalla Commissione europea nel giugno 2018, *Una definizione di IA: principali capacità e discipline* (*definizione elaborata ai fini dei documenti del gruppo*), aprile 2019, p. 1.

[32] *Ibidem*.

[33] *Ibidem*, p. 6.

paragrafo che segue si andrà a delineare puntualmente il perimetro di questo studio, concentrato soprattutto sull'impatto dei *big data* sui diritti fondamentali.

### *2.2. Dati e algoritmi come fattori condizionanti l'esercizio dei diritti fondamentali. I profili costituzionali della protezione dei dati personali*

Alla luce delle definizioni appena proposte, si può quindi passare ad analizzare l'impatto dei dati e degli algoritmi sull'esercizio dei diritti fondamentali.

Per comprendere appieno la portata della questione, è utile richiamare lo scenario ideato da Luciano Floridi per descrivere il nuovo ecosistema informativo in cui viviamo. Abbracciando la digitalizzazione, in molti Paesi si è passati da un'epoca "analogica" ad una nuova era storica – la così detta *hyperhistory* – un tempo in cui il benessere degli individui e della società materialmente dipendono delle tecnologie dell'informazione[34].

Oltre allo Stato – finora il principale detentore del potere informativo – a questa realtà si aggiungono altri agenti, in grado di esercitare, singolarmente o in modo congiunto, influenze e forze equivalenti se non maggiori a quelle di cui oggi sono in grado i Governi[35]. Se da un lato, infatti, i soggetti pubblici, sono ancora preposti alla raccolta e alla rilevazione di grandi quantità di contenuti (i dati territoriali, le schede anagrafiche, il casellario giudiziario, il registro delle imprese, solo per fare degli esempi) dall'altro oggi sono gli operatori privati – i già ricordati *tech giants* – a collezionare in modo continuo e subitaneo enormi flussi informativi, di qualsiasi natura.

---

[34] Il concetto di *hyperhistory*, descritto in questi termini, è stato inizialmente inaugurato in L. FLORIDI, *Hyperhistory and the Philosophy of Information Policies*, in L. FLORIDI (a cura di) *The Onlife Manifesto* op. cit., p. 52, e in seguito ripreso e ampliato in L. FLORIDI, *La quarta rivoluzione*, Milano, Cortina Ed., 2017.

[35] *Ibidem*, p. 55.

Queste due dimensioni dello sfruttamento dei *big data* – quella pubblica e quella privata – tuttavia, sono tutt'altro che aliene l'una all'altra. Se le imprese private, grazie agli *open data* sono in grado di sfruttare le risorse pubbliche per il raggiungimento di obiettivi economici che, pur portando anche un beneficio per la collettività, mirano pur sempre (e primariamente) ad un tornaconto economico, la pubblica amministrazione e le forze dell'ordine, nell'ambito delle loro attività, sempre più spesso ricorrono ai dati raccolti delle imprese private per arricchire le proprie risorse operative, ricorrendo a forme di partenariato per la realizzazione e la gestione dei più diversi progetti, dall'implementazione dell'internet delle cose nelle *smart cities*, all'introduzione dell'intelligenza artificiale per la pubblica amministrazione.

Alla luce di tutte queste considerazioni, appare quindi chiaro come il fenomeno dei *big data* e così la regolamentazione sull'utilizzo delle informazioni e delle tecnologie *data-intensive*, costituiscano un fattore decisivo rispetto alle possibilità di esercitare e godere dei tradizionali diritti fondamentali. Se si pensa a tutti i contesti in cui l'azione umana oggi è *intermediata* dall'utilizzo di un dispositivo digitale – dai semplici computer ai più sofisticati *wearable devices* – è facile intuire come, se l'azione umana si trasforma in termini computazioni, la struttura e la logica degli apparecchi di cui ci si avvale non solo determina un primo condizionamento (strumentale-funzionale) rispetto alle possibili alternative, ma grazie ai sottoprodotti informativi generati da tali operazioni semplici operazioni possono in seguito contribuire all'instaurarsi di condizionamenti ulteriori.

Ciò risulta quanto mai evidente anche nelle operazioni più banali: consultando un motore di ricerca i contenuti proposti sono condizionati dalle *queries* precedenti, così come dai risultati che rispetto ad esse sembrano essere stati di maggior interesse per l'utente. Lo stesso accade nell'utilizzo dei *social media*, in cui i vari *newsfeed* sono influenzati dall'attento monitoraggio del comportamento tenuto dall'intestatario del profilo nel corso del tempo. E questo non vale per tutti i contenuti: dalle notizie

proposte, ai contatti suggeriti, agli eventi messi in evidenza, fino ad intercettare le *sfumature* e le pieghe di contenuto apparentemente meno evidenti. La lista potrebbe continuare, allungandosi a dismisura tanti sono gli ambiti in cui possono registrarsi dinamiche simili a quelle accennate.

Grazie a queste considerazioni, si possono quindi cominciare ad intuire le implicazioni relative ai *diritti*. I condizionamenti cui si è appena fatto cenno, interferendo con i comportamenti, inevitabilmente finiscono infatti per incidere anche sul piano giuridico, fino a toccare il contenuto essenziale dei diritti fondamentali intercettati da queste intermediazioni tecnologiche. Basta guardare a quanto appena osservato per capire come dati e algoritmi possono influire non solo sulla corretta rappresentazione di sé – e così sul diritto alla riservatezza e all'autodeterminazione – così come su diverse libertà individuali, dalla libertà di espressione e informazione alla libertà di riunione e associazione, dalla libertà di impresa alla libertà di movimento. E di fronte a questa constatazione è stato compiuto, un primo passo – decisivo – transitando dalla realtà dei *fatti* alla dimensione dei *diritti*.

Invero, il rapporto tra il mondo del diritto e la sfera delle informazioni è stato affrontato già da tempo, seppur confrontandosi con una tecnologia di più modeste pretese. E più nello specifico, per quanto concerne il rapporto tra *dati* e *diritti*, una larga parte del discorso giuridico si è concentrato sull'elaborazione di una nuova serie di garanzie volte a tutelare lo sfruttamento e l'utilizzo dei dati personali.

Ci sarà tempo per approfondire l'*iter* storico che ha accompagnato lo sviluppo di questa disciplina. Quel che qui preme mettere in luce riguarda il fatto che il rapporto genetico e primigenio tra questi due settori – tecnologie dell'informazione e *data protection* – costituisce ancora il primo punto di riferimento quando si tratta di far fronte alle questioni legate alla rivoluzione delle informazioni, inclusi i *big data*.

Ed è soprattutto nel contesto europeo che questo confronto ha trovato maggiori sviluppi, anche in ragione della cultura giuridica maturata all'interno

dell'ordinamento comunitario rispetto a questi temi. Se infatti fin da principio le Comunità europee prima e in seguito l'Unione hanno fatto della protezione dei dati personali una delle normative di riferimento circa la tutela dei diritti nell'ambiente tecnologico-digitale, con la Carta di Nizza queste garanzie sono entrate definitivamente a far parte del patrimonio giuridico europeo, tanto da configurare un diritto fondamentale autonomo e a sé stante.

È impressionante constatare come lo sviluppo tecnologico abbia posto questa materia al centro della scena, sollevando importanti interrogativi sul destino di queste garanzie, così come sulla validità dei principi cui queste si ispirano. Se la protezione dei dati, infatti, costituisce il punto di partenza per ogni ulteriore riflessioni sul diritto in una realtà *data-intensive*, allo stesso tempo il potenziale di questo diritto in questo contesto rimane ancora in larga parte da indagare.

Garanzie tradizionalmente intese per tutelare la riservatezza e la sicurezza delle informazioni personali, oggi si trovano a dover fare i conti con un scenario profondamente mutato, in cui a queste preoccupazioni se ne aggiungono altre di ben diverso tenore. Non si può più concentrare l'attenzione sul solo rispetto della *privacy* – un nucleo di valori cui la protezione dei dati personali viene spesso sovrapposto – ma è necessario ampliare la prospettiva fino a definire il potenziale delle garanzie sul trattamento delle informazioni di circa tutti i diritti coinvolti dalla rivoluzione digitale.

Gli interrogativi che si aprono rispetto al problema appena accennato, dunque, sono molteplici. Per un verso, infatti, ci si trova di fronte all'urgenza di reinterpretare e ridefinire il quadro delle garanzie costituzionali per adattarne la forme e i contenuti alle esigenze del contesto digitale – e in questa operazione certo non passano in secondo piano quelle che sono le peculiarità delle singole esperienze, in linea con la tradizione del singolo ordinamento. Per contro, in seguito a questa progressiva migrazione verso l'alto del sistema di tutele, sempre più concentrate a livello comunitario, le prerogative degli Stati membri rispetto a questi temi risultano

sempre più temperate, poiché è inevitabile constatare che «ove si espande un sistema si restringe l'altro»[36].

Alla luce di queste considerazioni, dunque, è necessario sul rapporto tra questi due livelli di tutela – quello costituzionale nazionale e quello (para)costituzionale europeo – evidenziando i punti di contatto e di frizione che potrebbero emergere in questa nuova lettura dei diritti fondamentali in un contesto *data-driven*.

### 3. Il quesito di ricerca

In ragione di quanto appena detto, il quesito di ricerca attorno cui gravita questo studio può essere quindi delineato come segue:

> *In una realtà governata dai dati, di fronte all'esigenza di rideclinare in chiave digitale le garanzie ereditata della tradizionale costituzionale, in questo nuovo contesto qual è il ruolo del diritto alla protezione dei dati personali e della disciplina europea? E quali problemi possono emergere in questa progressiva "migrazione verso l'alto" del sistema di tutela?*

La formulazione è senz'altro articolata ma consente di proporre in termini coincisi *tutti* gli elementi che si andranno ad affrontare nel corso del lavoro. Analizzando attentamente i singoli punti, infatti, risulteranno chiari i termini del problema.

Il punto di partenza, come accennato in queste pagine, riguarda le perplessità accennate circa il rapporto tra dati e diritti: da un lato, si delinea una nuova forma di potere informativo (legato, per l'appunto, alla disponibilità e all'utilizzo dei *big data*) dall'altro, invece, consapevoli dell'impatto e delle conseguenze che derivano

---

[36] G. ZAGREBELSKY, *Costi europee e corti nazionali*, Resoconto della Relazione al Seminario dell'Osservatorio costituzionale della LUISS su *I mutamenti costituzionali in Italia nel quadro dell'integrazione europea*, 12 gennaio 2002, p. 1, come citato in F. SALOMONI, *Controlimiti, diritti con lo stesso* nome *e ruolo accentrato della Consulta*, in *federalismi.it*, 8/2019, p. 6.

dall'impego di queste tecnologie nella sfera giuridica dei soggetti interessati, si afferma l'esigenza di preservare il contenuto delle garanzie costituzionali anche in questo nuovo contesto.

L'accento cade quindi sui due piani tra i quali si snoda la riflessione: quello nazionale e quello europeo. Questioni tradizionalmente decise dai giudici nazionali, con il progresso della digitalizzazione, infatti, gradualmente si spostano – si polarizzano – verso l'alto, trovando come interlocutore principale il legislatore comunitario e la Corte di giustizia dell'Unione europea, sollevando così più di qualche interrogativo circa i diversi *modi decidendi* sulle questioni relative la portata dei diritti fondamentali.

Ed in quest'alveo si collocano le questioni relative alla protezione dei dati personali. Se tradizionalmente questa materia è sempre stata interpretata come una *disciplina* volta a tradurre sul piano della normativa di rango ordinario le garanzie necessarie alla tutela di alcuni diritti fondamentali (primo tra tutti, la *privacy*), a livello europeo oggi ci si confronta con una vero e proprio *nuovo diritto*, delineato come fattispecie autonoma e a se stante, sullo stesso piano di tutti gli altri. Se l'articolo 8 della Carta di Nizza, inquadrando subito la *data protection* come diritto fondamentale dell'Unione europea, certo aiuta a collocare il problema nell'alveo degli studi di diritto costituzionale, questa figura rappresenta ancora motivo di grandi perplessità. Non solo, infatti, la scelta di procedere lungo un doppio binario desta qualche interrogativo sul rapporto che oggi intercorre tra rispetto della vita privata e autoderminazione informativa. Il fatto che il diritto si concentri *solo* sui dati personali in una realtà fatta di *big data* solleva più di qualche problema, che nel corso del lavoro ci sarà modo di analizzare.

Si arriva, dunque, all'ultimo nodo da sciogliere: ossia il fatto che, soprattutto a motivo delle competenze sancite dell'art. 16 TFUE, attualmente le strategie di *data governance* – ossia i *corpora* normativi volti a disciplinare l'utilizzo dei dati nei diversi

settori – sono definite prevalentemente a livello europeo, spostando così importati decisioni di politica del diritto a livello sovrannazionale.

Alla luce di queste considerazioni, dunque, si spiega l'interrogativo. E questo lavoro mira di chiarire quale sia l'attuale funzione del diritto alla protezione dei dati personali, analizzando come questo è stato assimilato nel tempo dal diritto costituzionale nazionale e come promette di svilupparsi a livello europeo, evidenziando i possibili motivi di tensione all'interno di questo sistema di tutele integrato e multilivello.

A tal proposito, dunque, per chiarezza espositiva, il quesito di ricerca principale può essere letto come la somma di tre questioni minori:

1. *Come il diritto costituzionale interno ha affrontato le questioni relative al corretto trattamento dei dati per la tutela dei diritti fondamentali?*
2. *Come il diritto europeo ha contribuito all'affermazione di un nuovo diritto fondamentale alla protezione dei dati personali e quale ruolo giocano oggi le nuove competenze europee nella definizione della disciplina a riguardo?*
3. *Con l'avvento dei* big data *che risposte offre il diritto costituzionale europeo rispetto alla tutela dei diritti fondamentali coinvolti in questa rivoluzione tecnologica? E quali punti di contatto (e contrasto) possono emergere con il diritto costituzionale nazionale?*

### 4. Struttura e metodologia

Chiarite le premesse e il problema da cui origina il quesito di ricerca, lo studio si compone di tre diverse parti, cui si aggiungo questo primo capitolo introduttivo e l'ultima parte, dedicata alle conclusioni. Da un punto di vista argomentativo,

ciascuna di esse tende a dare risposta ad uno dei quesiti minori, così da poter infine delle considerazioni più sistematiche.

L'intento di questo paragrafo, è quello di delineare brevemente la struttura di ogni sezione e la metodologia utilizzata per lo sviluppo di ciascuna.

### *4.1. La protezione dei dati personali in Italia*

Il capitolo 2 si concentra sull'evoluzione della disciplina sulla protezione dei dati personali in Italia, analizzando soprattutto i fondamenti costituzionali di questa materia. L'obiettivo è quello di chiarire come la dottrina, la giurisprudenza e – in ultima – il legislatore nel tempo abbiano affrontato le questioni relative alla tutela dei diritti in un ecosistema informativo in evoluzione, adattando il precedente sistema di garanzie alle caratteristiche del contesto digitale.

L'analisi si concentra soprattutto sugli argomenti e le tecniche normative utilizzati per promuovere questa graduale innovazione della precedente tradizione. Soprattutto, preme mettere in evidenza come, in queste operazioni, i giuristi nazionali abbiano gradualmente assimilato il portato delle esperienze maturate in altri ordinamenti. L'attenzione, dunque, si concentra su due aspetti: il rapporto tra diritti e informazioni (e così, inevitabilmente, sul graduale riconoscimento del diritto alla riservatezza) e il rapporto tra diritto costituzionale italiano ed europeo, mettendo ben in luce i punti di contatto e i tratti di originalità che connotano l'esperienza interna.

Quanto alla metodologia, in questa prima parte si è seguito per lo più l'approccio tipico degli studi di diritto costituzionale. Dopo una prima panoramica sull'evoluzione storica della disciplina in ambito europeo, ci si è concentrati soprattutto sulla giurisprudenza e sulla dottrina costituzionale interna, analizzando soprattutto quanto previsto dalla prima legge sulla *privacy* (la n. 675 del 1996), le

novità apportate dal c.d. Codice privacy (d.lgs. n. 196 del 2003) e, da ultimo, la riforma introdotta d.lgs. n. 101 del 2018.

### *4.2. La protezione dei dati personali come diritto fondamentale*

Il capitolo 3 esamina il percorso che ha portato all'affermazione di uno specifico diritto fondamentale europeo alla protezione dei dati personali, e così all'affermazione di nuove specifiche competenze a livello comunitario. Analizzando le tappe che segnano il passaggio dalla direttiva "madre" (dir. 95/46) al nuovo regolamento (reg. 679/2016), l'intento è quello di chiarire come abbia inciso la "costituzionalizzazione" di questa materia in ambito europeo e come dunque il sistema di garanzie elaborato da Bruxelles oggi dialoghi con quello in precedenza istituto dagli Stati membri.

Si andranno a delineare i motivi storici che hanno portato alla graduale europeizzazione della disciplina sulla protezione dei dati personali. Si analizzeranno i lavori preparatori che hanno portato al primo "pacchetto privacy". In ciascun passaggio si tenterà di mettere in luce come i cambiamenti istituzionali abbiano progressivamente contribuito ad una lettura "costituzionalmente orientata" di questa disciplina, fino ad ipotizzare la statuizione di un autonomo diritto fondamentale.

In questa seconda parte, dunque, si è ricorsi per lo più ad approccio di tipo storico-evolutivo, analizzando i passaggi che hanno portato al delinearsi dell'attuale quadro costituzionale e normativo a livello europeo. Si prenderanno in esame i contenuti delle principali normative in materie soffermandosi soprattutto sulla direttiva primigenia (la già ricordata dir. 95/46), il regolamento sul protezione dei dati personali nell'attività delle istituzioni europee (reg. 2001/45), la direttiva sulla c.d. *e-privacy* (dir. 2002/58) e, da ultimo, l'ormai annullata normativa sulla c.d. *data retention* (dir. 2006/24). Si analizzerà quindi il percorso storico che ha portato

all'introduzione dell'art. 8 CDFUE, al riconoscimento della Carta come parte integrante del diritto dei Trattati e alla riforma dell'art. 16 TFUE. Si dedicherà quindi particolare attenzione allo studio dei contenuti essenziali del reg. 679/2016, con alcuni accenni alla nuova strategia di *data-governance* europea.

### *4.3. Diritti fondamentali e big data*

Il capitolo 4, infine, affronta le questioni legate alla diffusione dei *big data analytics* e, con essi, dell'intelligenza artificiale, focalizzando l'attenzione soprattutto sui sistemi di decisione automatizzata e di profilazione. L'intento di queste pagine è quello di evidenziare le aree critiche, in cui si riscontrano maggiormente i segni di quella crisi di identità che – come si accennava – oggi interessa il diritto alla protezione dei dati personali e la relativa disciplina.

A tal proposito, indagando soprattutto il rapporto tra dati e diritti fondamentali tra diritto nazionale e diritto europeo, sono stati scelti quattro principali nodi tematici. In primo luogo, si affronterà il rapporto tra certezza del diritto, dati personali e *big data,* approfondendo soprattutto i problemi che emergono quanto ai rischi di un interpretazione sovradimensionata della disciplina sulla protezione dei dati personali nel contesto attuale, fino a fare di questo diritto una nuova «teoria del tutto». Seguirà quindi un'attenta indagine incentrata sul trittico Stato di diritto-*privacy*-*big data*, qui analizzando il rapporto tra le tradizionali garanzie dello stato di diritto e il rapporto tra *privacy* e *big data*, analizzando soprattutto il rapporto tra diritto europeo e diritto nazionale nell'utilizzo dei dati personali per finalità di pubblico interesse. Si passerà quindi ad approfondire il tema relativo ai diritti fondamentali, i *big data* e la valutazione del rischio; partendo da una prima mappatura dei diritti oggi coinvolti nell'utilizzo dei *big data*, si analizzeranno le tecniche di bilanciamento utilizzate dai giudici europei nell'utilizzare il "parametro"

fornito dall'art. 8 della Carta, soprattutto in funzione delle metodologie volte ad una preventiva valutazione del rischio. Infine ci si concentrerà sul principio di trasparenza, focalizzando l'attenzione sulle premesse necessarie a promuovere un utilizzo "costituzionalmente orientato" dei *big data*; un'ultima parte in cui, alla luce delle considerazioni svolte in precedenza, ci si concentrerà soprattutto sulla dimensione rimediale, indagando come la normativa europea affronta i problemi relativi alla trasparenza nell'utilizzo dei *big data*. Ci si soffermerà soprattutto sull'opportunità di riconoscere nuovi (e fondamentali?) diritti ad una spiegazione o ad una "leggibilità" delle decisioni assunte sulla base dei relativi sistemi di calcolo, valutando anche le alternative elaborate a livello nazionale.

Come facile intuire, per svolgere quest'analisi si è ricorsi soprattutto allo studio della giurisprudenza, e così al metodo casistico. Per chiarire infatti la portata della neo-introdotta normativa, si sono esaminate soprattutto quelle decisioni che hanno segnato un significativo avanzamento della dottrina costituzionale nazionale ed europea. In particolare, si sono considerate soprattutto le sentenze che si sono soffermate su questioni o hanno sviluppato argomenti utili a comprendere i possibili sviluppi dell'attuale quadro delle garanzie a tutela dei diritti fondamentali. Alla luce di queste considerazioni, dunque, nell'ultima sezione di questo scritto, si sono formulate alcune prime conclusioni, evidenziando gli ambiti in cui maggiormente si avverte il rischio di uno scontro tra il costituzionalismo digitale nazionale e lo sviluppo di un parallelo percorso a livello europeo, proponendo alcune possibili raccomandazioni.

# Capitolo 2

## La protezione dei dati personali in Italia
*L'evoluzione della disciplina e i suoi fondamenti costituzionali*

### 1. Introduzione

Nell'ecologia generale di questo studio, questo capitolo si propone di affrontare il problema posto dal primo sotto-quesito di ricerca, ossia come il diritto costituzionale interno abbia affrontato le questioni relative al corretto trattamento dei dati personali.

L'obiettivo è quello di evidenziare l'approccio adottato prima dalla Consulta e poi dal legislatore per delineare i principi posti a fondamento di questa disciplina, evidenziando soprattutto gli influssi sortiti dal diritto europeo e straniero nell'evolversi di questo processo. Seguendo questa traiettoria, al termine, sarà possibile porre le debite premesse per passare all'analisi del quadro normativo comunitario, avendo a mente soprattutto il "cambio di rotta" registrato nella giurisprudenza costituzionale più recente nei rapporti con quest'ordinamento.

### 2. La protezione dei dati personali come una normativa di chiara «discendenza comunitaria». Alcune premesse guardando al diritto europeo

Guardando alla disciplina sulla protezione dei dati personali, la Corte costituzionale italiana non ha esitato ad ammettere come questa normativa abbia

una chiara «discendenza comunitaria»[37]. Nel nostro ordinamento, infatti, a differenza di quanto verificatosi altrove, le questioni legate alla tutela di tali informazioni sono state affrontate con un certo ritardo. Ed è per questo motivo che l'esperienza interna deve molto all'influenza dei principi e dei modelli elaborati in altri contesti, da cui i giudici e il legislatore hanno sapientemente attinto.

Il punto di partenza, dunque, è proprio questo. Prima di analizzare come si siano sviluppati lo studio e la regolamentazione di questa materia in Italia, si andranno a ripercorrere le principali tappe dell'evoluzione di questo diritto in altri Stati e in Europa.

La letteratura italiana e straniera[38], nel tempo, si è già soffermata ampiamente su questi profili storico-comparatistici, ragion per cui, in questa sede, si procederà in modo diverso. L'intento non è quello di analizzare puntualmente i singoli atti né, tanto meno, cogliere appieno le peculiarità di ciascun contesto. L'obiettivo, piuttosto, è quello di far emergere per linee generali, i problemi cui questa disciplina si propone di rispondere e le soluzioni elaborate a livello nazionale e sovranazionale per estendere le tradizionali garanzie a favore dei diritti fondamentali di fronte allo sviluppo delle nuove tecnologie dell'informazione.

---

[37] Corte cost., sent. n. 271/2005, in specie, §§ 2 e 3 del *Considerato in diritto.*

[38] Si rimanda, *ex multis*, a F.W. HONDIUS, *Emerging Data Protection in Europe*, cit.; D.H. FLAHERTY, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*, Chapel Hill, University of North Carolina Press, 1989; C.J. BENNETT, *Regulating Privacy. Data Protection and Public Policy in Europe and the United States,* Ithaca-Londra, Cornell University Press, 1992; G. BUTTARELLI, *Banche dati e tutela della riservatezza. La* privacy *nella Società dell'Informazione*, Milano, Giuffrè, 1997; D. VANNI, *La protezione dei dati personali in prospettiva comparatistica*, Roma, Aracne, 2012; G. GONZÁLEZ FUSTER, *The emergence of data protection as a fundamental right of EU*, Cham-Heidelberg-New York-Dordrecht-Londra, Springer, 2014.

### *2.1. Le prime "leggi sui dati" in Europa*

Cominciando a tracciare i profili storici della disciplina sulla protezione dei dati personali bisogna fare un salto all'indietro, andando ad analizzare gli sviluppi che, in principio, hanno caratterizzato le prime leggi in materia; quelle approvate in Svezia, Germania e Francia nel corso degli anni Settanta[39].

A ben vedere, questi primi "esperimenti"[40] hanno affrontato temi e questioni che vanno ben oltre la sola protezione dei dati. Nel secondo dopoguerra, infatti, avevano cominciato a diffondersi i primi computer, e i nuovi elaboratori elettronici erano stati rapidamente adottati non solo dalla pubblica amministrazione, ma anche dalle grandi società private, rivoluzionando così la gestione di flussi informativi in modo trasversale e su vasta scala.

Sul piano del diritto, questa rapida diffusione dell'informatica non ha mancato di sollevare questioni, relative peraltro a diversi aspetti relativi a queste tecnologie. Così, da un lato, vi erano i problemi legati ai computer in quanto tali, come, ad esempio, la tutela della proprietà intellettuale rispetto ai *software* o la fungibilità tra documenti cartacei e copie digitali. Dall'altro, invece, quelli relativi all'utilizzo dei nuovi elaboratori e al loro impatto sulla sfera dei diritti[41].

---

[39] In ordine cronologico, la prima disciplina sul trattamento elettronico dei dati è quella del *Land* tedesco dell'Assia, che risale al 1970. Sebbene si tratti di una legge statale approvata in un ordinamento federale, è a quest'atto che si deve la stessa nozione di protezione dei dati, elaborata proprio in quell'occasione con l'espressione *Datenschutz*. Una dicitura di tenore analogo è quella che si trova nella legge svedese approvata di lì a poco, nel 1973, con il titolo, appunto, di *Datalag* (letteralmente: *legge sui dati*). Qualche anno più tardi (e con un'impostazione diversa) segue, nel 1978, la promulgazione della legge francese, questa volta incentrata, più che sui soli dati personali, sull'utilizzo dell'informatica in generale (*Loi relative à l'informatique, aux fichiers at aux libertés du 6 janvier 1978*).

[40] Da più parti, soprattutto guardando alla legge svedese – il primo grande esempio per una disciplina sistematica di questa materia – queste prime leggi sono state definite, appunto, degli esperimenti; dei primi tentativi per rispondere ad un problema assolutamente nuovo. Circa la definizione di "esperimenti", v. J. BING, *A Comparative Outline of Privacy Legislation*, in *Comparative Law Yearbook*, 2, 1978, p. 150, cit. in C.J. BENNETT, *Regulating Privacy*, cit., p. 60, n. 26.

[41] F.W. HONDIUS, *Emerging Data Protection in Europe*, cit. pp. [6-8] e 19.

La protezione dei dati personali, evidentemente, rientra nel secondo di questi insiemi. E tuttavia è interessante notare come, in tal senso, ancora prima di parlare di un *nuovo diritto*, affrontando questo tema sia stato necessario far fronte ad un *nuovo problema di diritto*[42].

La prassi di raccogliere e gestire grandi quantità di informazioni sulla vita privata e professionale delle persone era ormai invalsa da molto tempo, ma l'utilizzo dell'informatica certo prometteva di incrementare i vantaggi connessi a questo tipo di operazioni (e, con essi, le relative derive patologiche)[43]. A partire da quel momento, infatti, da un punto di vista tecnico e socio-economico, i computer smettono di essere considerati dei meri *calcolatori*, utili soprattutto in ambito statistico, ma diventano dei veri e propri *elaboratori*, capaci di analizzare ed aggregare diverse basi di dati, offrendo risultati e contenuti inediti.

E così, se la pubblica amministrazione aveva cominciato ad utilizzarli per gestire i dossier sui singoli cittadini spaziando negli ambiti più diversi – dalle prestazioni previdenziali agli schedari di polizia – in ambito privato si iniziano ad adottare questi sistemi per verificare la solvibilità creditizia, per valutare il rischio assicurativo, piuttosto che per fini di profilazione commerciale.

In questo modo, dunque, le nuove tecnologie appena inaugurate non solo hanno contribuito a consolidare nuove posizioni di potere legate alla gestione delle informazioni, ma la disponibilità di così ingenti quantità di dati sulla vita dei singoli comincia a sollevare questioni inedite circa la tutela della sfera personale e dell'autodeterminazione individuale[44].

---

[42] *Ibidem*, p. 18. Attestazioni analoghe si rinvengo comunque anche in A.F. WESTIN, *Privacy and Freedom*, New York, Athenaeum, 1970 (edizione originale 1967), chiaramente con delle riflessioni concentrate sul contesto nord-americano.

[43] S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, Il Mulino, 1974, pp. [12-16].

[44] Un'analisi, tutto sommato, condivisa da diversi autori. Cfr. F.W. HONDIUS, *Emerging Data Protection in Europe*, cit. p.[8-10]; S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, pp. [28-33]; C.J. BENNETT, *Regulating Privacy*, cit., pp. [14-37].

Quelli appena accennati, nel giro di pochi anni, diventeranno problemi assai diffusi, comuni a diversi ordinamenti in Europa come altrove. Tuttavia, quello che contraddistingue l'esperienza europea rispetto a quella maturata in altri ambienti è il fatto di affrontare tali scenari assecondando un approccio molto tecnico, orientato verso un'attenta regolamentazione pratica delle attività di trattamento piuttosto che verso una semplice rilettura della *privacy*[45].

Ciò premesso, ad uno sguardo d'insieme, considerata la pluralità di esperienze che hanno preso piede nel contesto europeo, non si può fare a meno di notare come in esse spicchi un elemento comune. A fondamento delle diverse discipline, infatti, ovunque si trovano alcuni valori centrali e comunemente condivisi: la dignità dell'uomo, la libertà personale, la riservatezza, l'autonomia e, più in generale, la tutela dei diritti fondamentali. Esaminando però trasversalmente i contenuti di queste prime normative si scorge come all'interno delle singole esperienze si delineano dei tratti peculiari, dettati dalle diverse sensibilità rispetto ai problemi.

In tal senso, si può tentare una prima essenziale mappatura dei problemi. Guardando al contesto austriaco-tedesco, ad esempio, erano emersi soprattutto due ordini di questioni: da un lato, la tutela della trasparenza e il controllo sociale sull'utilizzo delle informazioni; dall'altro le garanzie di correttezza e regolarità dei sistemi di calcolo[46]. In Svezia, invece, si erano posti problemi ben diversi poiché era

---

[45] Rispetto a questo punto, va chiarito che mentre parte della dottrina utilizza i due concetti – *privacy* e *data protection* – come se fossero sinonimi, secondo l'impostazione di stampo americano (cfr. A.F. WESTIN, *Privacy and Freedom*, cit.; D.H. FLAHERTY, *Protecting Privacy in Surveillance Societies*, cit.) altri autori, più affini al metodo comparatistico, guardando al contesto europeo hanno evidenziato alcune differenze non solo sul piano terminologico, soffermandosi sul distinguo tra *privacy* e *data protection*, ma anche analizzando le analogie e le differenze i vari modelli di tutela elaborati nei diversi contesti in materia di riservatezza e protezione dei dati (cfr. C.J. BENNETT, *Regulating Privacy*, cit., pp. [12-14]; G. GONZÁLEZ FUSTER, *The emergence of data protection as a fundamental right of EU*, cit. pp. [27-48] (circa il concetto di *privacy* negli Stati Uniti e in Europa) e pp. [56-61] (circa l'emergere del concetto di protezione dei dati)).

[46] V. MAYER-SCHÖNBERGER, *Generational Development of Data Protection in Europe*, in P.E. AGRE, M. ROTENBERG (a cura di), *Technology and Privacy: The New Landscape*, Cambridge(MA)-Londra, MIT Press, 1997, pp. 221-222. Le esperienze sviluppate nell'ambito del diritto di area tedesca vanno analizzate alla luce di due premesse essenziali: da un lato, si tratta di ordinamenti

accaduto che, giovandosi del diritto di accesso ai documenti pubblici, i soggetti privati avessero cominciato ad accumulare informazioni pressoché illimitate sull'intera popolazione nazionale– un'operazione, chiaramente, resa ancor più agile grazie alla digitalizzazione degli archivi[47]. Il legislatore francese, invece, aveva dimostrato preoccupazioni di più ampio respiro, legate alla tutela delle libertà e diritti fondamentali dei cittadini rispetto all'utilizzo dell'informatica in generale,

---

strutturati in forma federale; dall'altro, soprattutto nella Repubblica federale tedesca (RFG), l'informatica era divenuta subito un mercato trainante, con una rapida digitalizzazione della pubblica amministrazione e del settore privato. Per questi motivi, in tale contesto, emergono soprattutto questioni di natura istituzionale La pubblica amministrazione aveva rapidamente convertito la propria attività ai computer e, con l'intento di realizzare un ampio sistema di *welfare,* la gestione di corpose quantità di informazioni rappresentava un'esigenza imprescindibile. D'altro canto, se a livello federato si erano approvate delle prime leggi sulla protezione dei dati, la mancanza di una normativa federale rischiava di frustrare il risultato di simili iniziative; e ciò trascurando le conseguenze di simili prassi sugli equilibri politici e costituzionali tra governi e parlamenti locali e centrali. In tal senso, dunque, non solo ci è inizialmente attivati per garantire la certificazione e la regolarità dei sistemi di calcolo come prima garanzia a tutela dei cittadini ma si sono anche previste specifiche condizioni di accesso e controllo sull'operato delle pubbliche amministrazioni nei diversi livelli del sistema statale. Cfr. F.W. HONDIUS, *Emerging Data Protection in Europe*, cit., pp. [23-27] (Austria); pp. [34-39] (RFG); D.H. FLAHERTY, *Protecting Privacy in Surveillance Societies*, cit., pp. 21 ss. (RFG); C.J. BENNETT, *Regulating Privacy*, cit., pp. 74 ss. (RFG); G. GONZÁLEZ FUSTER, *The emergence of data protection as a fundamental right of EU*, cit. pp. [56-58], 60-61 (RFG); p. 67 (Austria).

[47] Fin dal 1776, in Svezia, è garantito l'accesso ai documenti della pubblica amministrazione; una prerogativa di portata generale che da allora trova chiaro riconoscimento sul piano costituzionale. Questo diritto può essere esercitato con pochissime eccezioni tanto dai privati cittadini, quanto dai soggetti istituzionali, in ossequio ai principi di trasparenza e *open government* che tradizionalmente informano tale ordinamento. Con la digitalizzazione della pubblica amministrazione e dei suoi archivi, tuttavia, si era registrata una situazione paradossale. I singoli individui, mancando della strumentazione necessaria ad ottenere una copia digitale della documentazione, spesso si trovavano impediti nell'esercizio di tale diritto; per contro, le grandi società, ben potendo disporre di tali sistemi, potevano ottenere informazioni illimitate su praticamente l'intera popolazione nazionale, riutilizzando poi tali contenuti per il loro profitto. Messi a fuoco questi rischi, dunque, ci si era attivati per introdurre una nuova serie di garanzie che, pur non facendo venir meno i poteri di controllo dei cittadini sull'operato della pubblica amministrazione, potessero comunque porre dei limiti e delle condizioni a simili prassi, evidentemente patologiche anche rispetto alla natura dell'istituto. Cfr. F.W. HONDIUS, *Emerging Data Protection in Europe*, cit., pp. 44 ss.; R. PAGANO, *Tutela dei dati personali: evoluzione della legislazione europea e stato del dibattito*, in *Informatica e diritto*, 1986, pp. 83 ss.; D.H. FLAHERTY, *Protecting Privacy in Surveillance Societies*, cit., pp. 93 ss.; C.J. BENNETT, *Regulating Privacy*, cit., pp. 60 ss.; G. GONZÁLEZ FUSTER, *The emergence of data protection as a fundamental right of EU*, cit.. pp. 58-59.

prefigurando così un approccio più sistematico, volto a declinare le tradizionali garanzie a favore della *liberté* anche nei diversi contesti di utilizzo dell'*informatique*[48].

La priorità dichiarata di queste nuove normative, dunque, è stata quella di disciplinare l'utilizzo delle tecnologie in modo tale da salvaguardare i diritti e le libertà della persona, così come l'equilibrio tra poteri pubblici e privati nella gestione delle informazioni personali. Così facendo, si sono affermate dapprima una serie di misure di natura tecnico-amministrativa, come le procedure di autorizzazione per l'istituzione di nuove banche dati o i sistemi di certificazione dei programmi. A queste, poi, han fatto seguito nuovi di meccanismi volti a promuovere un controllo politico e sociale sull'utilizzo dei dati, favorendo soprattutto l'accessibilità dei dati anche a beneficio dei singoli individui. Si sono quindi aggiunti alcuni nuovi diritti, in questo caso volti ad assicurare all'interessato la possibilità di opporsi ad alcune tipologie di trattamento e di ottenere la rettifica sulle informazioni erronee. Infine, negli anni a venire, traendo spunto soprattutto dalla figura storica dell'*ombudsman* svedese, si coglie pressoché ovunque l'opportunità di istituire nuove autorità indipendenti, orientando così il sistema di tutela dei diritti verso un modello di stampo amministrativistico.

---

[48] In Francia l'evoluzione della disciplina ha conosciuto un percorso un po' diverso rispetto a quello di altre realtà. Si tratta anche in questo caso di una legislazione preventiva, che però, invece che concentrarsi sulla sola disciplina dei dati personali, affronta il tema in chiave generale introducendo una disciplina per allineare l'utilizzo dell'informatica agli obiettivi e ai valori sociali. Il fattore scatenante, in particolare, erano stati alcuni articoli apparsi sul quotidiano *Le Monde* nel 1974 nei quali, descrivendo la recente proposta di istituire una banca dati centrale nazionale (il c.d. progetto *SAFARI*), si prospettavano possibili rischi per le libertà individuali legati all'utilizzo dei dati personali. Il disegno di legge proposto due anni dopo dal Governo Mitterand, prospettava dunque una lettura istituzionale della disciplina, in cui lo Stato, così come in altri ambiti, si sarebbe fatto ultimo garante dei diritti e delle libertà dei cittadini, disciplinando per intero il settore delle ICT. Il tratto che caratterizza questa iniziativa è, dunque, proprio l'ampia portata delle sue previsioni; una disciplina che, quanto meno formalmente, va ben oltre i concetti di *privacy* e protezione dei dati personali. F.W. HONDIUS, *Emerging Data Protection in Europe*, cit., pp. 31 ss.; G. ALPA, *Privacy e statuto dell'informazione (il* privacy act 1974 *e* la Loi relative à l'informatique, aux fichiers at aux libertés *n. 78.17 del 1978)*, in M. BESSONE, G. GIACOBBE (a cura di), *Il diritto alla riservatezza in Italia e ed in Francia,* Padova, Cedam, 1988, pp. 314 ss.; D.H. FLAHERTY, *Protecting Privacy in Surveillance Societies*, cit., pp. 165 ss.; S. RODOTÀ, *Tecnopolitica*, Roma, Laterza, 2004 pp. 150 ss.; G. GONZÁLEZ FUSTER, *The emergence of data protection as a fundamental right of EU*, cit., pp. 61 ss.

Alla luce di questi rilievi, si osserva quindi come storicamente la protezione dei dati personali si sia affermata grazie ad una serie di tentativi volti ad improntare i rapporti istituzionali in qualsiasi modo interessati dal trattamento dei dati ai tradizionali valori di lealtà e correttezza, nell'ottica di salvaguardare così le libertà e i diritti fondamentali e i valori democratici del pluralismo anche in un contesto informatizzato.

Come si è visto, si possono rintracciare in ognuna degli elementi che poi sono divenuti ricorrenti, tanto da consolidarsi nel tempo come componente essenziale del modello di protezione comunitaria. A questo processo di mutua assimilazione hanno concorso diversi fattori[49], tra i quali merita attenzione soprattutto l'opera di coordinamento esercitato a livello sovranazionale da diverse organizzazioni impegnate in diversi ambiti; tema che verrà subito approfondito del prossimo paragrafo.

### *2.2. La Convenzione 108/1981 e il ruolo della Corte EDU*

In concomitanza con gli sviluppi accennati poc'anzi, il tema della protezione dei dati personali è stato affrontato anche a livello internazionale, analizzando da più

[49] Analizzando i punti di convergenza e divergenza tra il sistema di tutela elaborato negli Stati Uniti e quelli invece fioriti nel contesto europeo, si è osservato come, effettivamente, il tema dell'*informational privacy* o, che dir si voglia, *data protection* documenti in modo lampante una rapida e proficua circolazione di modelli. Indagando le ragioni di queste somiglianze, si è riscontrato come queste possano essere ricondotte essenzialmente (*a*) alla novità delle questioni giuridiche poste dallo sviluppo dell'informatica; (*b*) ad una forte propensione all'emulazione/imitazione degli strumenti e degli espedienti adottati in altri ordinamento (e, con questo, un grande approfondimento comparatistico); (*c*) al rapido istaurarsi di una solida rete internazionale di relazioni e confronto tra gli esperti del settore a livello nazionale; (*d*) agli espliciti intenti di armonizzazione della disciplina promossi a livello sovranazionale e, ultimo ma non ultimo, (*e*) l'inevitabile contatto con le altre discipline da parte degli operatori coinvolti su scala internazionale nel mercato delle nuove tecnologie. Cfr. C.J. BENNETT, *Regulating Privacy*, cit., spec. pp. [3-5].

punti di vista i rischi per la tutela dei diritti fondamentali e gli aspetti legati allo sfruttamento economico delle informazioni[50].

Considerando come l'utilizzo dei computer in quegli anni si fosse fatto strada in contesti sempre più diversi, spaziando dal settore dell'istruzione a quello della sanità, dall'amministrazione carceraria alle assicurazioni, si era avvertita ovunque l'esigenza di promuovere una rapida conversione digitale, ben intuendo i vantaggi economici e sociali legati allo sviluppo di queste tecnologie[51].

Trattandosi di un mercato tendenzialmente globale, da un lato, si era creata subito una fitta rete di relazioni commerciali tra i diversi operatori, e questo a dispetto del fatto che questi potessero essere dislocati in Stati e giurisdizioni differenti. Dall'altro, lo sviluppo delle telecomunicazioni e dell'informatica aveva reso ancor più facile lo scambio di dati tra i diversi *partners*, consentendo così una sempre rapida condivisione del patrimonio e dei flussi informativi, anche per fini e utilità inaspettate.

A fronte di tutto ciò, si era consapevoli che queste trasformazioni avrebbero avuto importanti implicazioni sul piano sociale, così come sui diritti delle persone coinvolte.

In tal senso, se l'approvazione delle prime leggi sulla protezione dei dati era stata in qualche modo avvertita come una sorta di conquista culturale necessaria, ora il fatto che la normativa potesse cambiare da uno Stato a un altro, rappresentava un ostacolo significativo alla circolazione transfrontaliera dei dati, così come allo sviluppo dell'economia di settore. Per contro, però, visto il considerevole aumento dei flussi informativi, lasciare tali attività completamente deregolamentate sarebbe

---

[50] F.W. HONDIUS, *Emerging Data Protection in Europe*, cit., pp. [55-57].

[51] Sui profili relativi all'ambivalenza dell'utilizzo delle tecnologie informatiche, v. S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, cit., pp. 9 ss. Considerazioni analoghe anche in A.F. WESTIN, *Privacy and Freedom*, cit.; A.F. WESTIN, M.A. BAKER, *Data banks in a Free Society*, New York, Quadrangle Books, 1972. Rispetto agli sviluppi più recenti, soprattutto a livello sovranazionale, v. BUTTARELLI, *Banche dati e tutela della riservatezza*, cit., pp. 8 ss.

risultato assolutamente inaccettabile, soprattutto quando questo avesse comportato una legittimazione delle attività più pregiudizievoli per i diritti degli interessati[52].

Così, a partire dagli anni Sessanta, vi erano stati diverse occasione per un confronto allargato su questi temi, coinvolgendo nelle diverse proposte una pluralità di attori istituzionali, europei e non solo. L'obiettivo comune a queste iniziative era, innanzitutto, quello di promuovere un dialogo sulle questioni legate alla protezione della *privacy* e dei dati personali, sensibilizzando i legislatori nazionali e facilitando la circolazione dei diversi modelli di tutela[53]. A questo scopo ideale, tuttavia, se ne aggiungeva uno ben più rilevante, ossia l'intento di trovare delle regole condivise a livello sovranazionale per conciliare la libera circolazione delle informazioni con la tutela dei diritti fondamentali[54].

Dei tanti lavori prodotti su questo tema, tuttavia, due in particolare, più degli altri, hanno avuto un ruolo essenziale nella definizione del futuro *framework* normativo europeo. Si tratta delle *Linee Guida sulla Privacy* pubblicate dall'OECD nel 1980 e la Convenzione sulla protezione delle persone rispetto al trattamento

---

[52] P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione europea*, Milano, Giuffrè, 2002, pp. 49 ss.

[53] Ricostruendo brevemente la cronologia di questi eventi, inizialmente una prima conferenza sul tema *privacy* digitalizzazione fu organizzata nel 1967 nell'ambito della *Nordic Conference* promossa dall'*International Commission of Jurists* svedese. Analogamente, negli stessi anni, a Teheran nel 1969, le Nazioni Unite, in occasione della Conferenza Internazionale sui diritti umani, avevano ulteriormente approfondito l'argomento, analizzandolo soprattutto alla luce della digitalizzazione degli archivi pubblici. A quelle prime occasioni era seguita quindi la pubblicazione dello studio *Privacy and the Law* edito, questa volta, dalla sezione britannica *dell'ICJ* (con un'apposita sezione dedicata al tema *Computer and the Law*) nel 1970. A tali iniziative si somma quanto promosso in seno all'Organizzazione per la cooperazione e lo sviluppo economico (OECD) a partire dal 1978, con la nomina di un Gruppo di esperti preposti all'elaborazione delle nuove linee guida e i lavori avviati nel 1968 dal Consiglio d'Europa che avrebbero poi portato alla proclamazione della Convenzione n. 108/1981. Per una ricostruzione sistematica, si rinvia a G. GONZÁLEZ FUSTER, *The emergence of data protection as a fundamental right of EU*, cit., pp. 39 ss. e 75 ss; G. BUTTARELLI, *Banche dati e tutela della riservatezza*, cit., pp. 28 ss.

[54] Si temeva, infatti, che al frammentazione normativa e la particolare sensibilità dimostrata rispetto a questo tema in alcuni ordinamenti potesse falsare gli equilibri del futuro mercato delle informazioni, creando delle aree di ristagno tra «paradisi informatici» e «protezionismo dei dati». Cfr. G. BUTTARELLI, *Banche dati e tutela della riservatezza*, cit., p. 5.

automatizzato di dati a carattere personale (la c.d. Convenzione n. 108), approvata in seno al Consiglio d'Europa l'anno successivo, nel 1981.

Pensando a come in seguito è venuta ad affermarsi la disciplina sulla *data protection*, questi documenti risultano di particolare in importanza per almeno due ordini di motivi.

Da un punto di vista terminologico, grazie ad essi nel dibattito politico europeo comincia a farsi strada il moderno concetto di *privacy*, richiamando fortemente gli argomenti e le teorie elaborati negli Stati Uniti soprattutto nell'opera di Alan Westin. Nel diritto continentale, infatti, vi erano già delle figure giuridiche preposte alla tutela della sfera privata e dell'autonomia individuale, le quali però erano state declinate nei vari ordinamenti secondo le diverse sensibilità, ricorrendo a concetti *Privatsphäre, vie privée*, *intimidad* o *riservatezza*[55]. Nell'ambito di questi studi invece, cercando un punto di compromesso tra i diversi approcci a questa materia, si stabilisce un collegamento diretto tra la protezione dei dati personali e la tutela della *privacy* come diritto fondamentale, veicolando così l'idea che questa disciplina fosse destinata ad essere più che una mera normativa tecnica, attribuendole un'implicita valenza costituzionale[56].

---

[55] Rispetto all'evoluzione di questi concetti, in chiave comparativa, rispetto al diritto di area tedesca si rimanda a: A. FIGONE, *Il diritto alla riservatezza dell'ordinamento francese,* M. BESSONE, G. GIACOBBE (a cura di), *Il diritto alla riservatezza in Italia e ed in Francia,* cit., pp. 572 ss.; rispetto al diritto italiano: F. BILOTTA, *L'emersione del diritto alla privacy*, in A. CLEMENTE (a cura di), *Privacy*, Padova, Cedam, 1999; NIGER, *Le nuove dimensione della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, Cedam, 2006,: rispetto al diritto spagnolo: G. FAMIGLIETTI, *Il diritto alla riservatezza o la riservatezza come diritto. Appunti in tema di riservatezza ed* intimidad *sulla scorta della giurisprudenza della Corte costituzionale e del* Tribunal Constitucional, in A. D'ALOIA (a cura di), *Biotecnologie e valori costituzionali. Il contributo della giurisprudenza costituzionale*, Torino, Giappichelli, 2005. Per una panoramica più ampia e trasversale si rimanda inoltre a A. DI MARTINO, *I profili costituzionali della privacy negli Stati Uniti e in Europa*, Jovene, Napoli, 2017, *passim* (profili giuridico-costituzionali) e a G. GONZÁLEZ FUSTER, *The emergence of data protection as a fundamental right of EU*, cit., pp. 21 ss. (profili giuridico-linguistici).

[56] P. DE HERT, S. GUTWIRTH, *Data Protection in the Case Law od Strasbourg and Luxemburg: Constitutionalisation in Action*, in S. GUTWIRTH ET AL (a cura di), *Reinventing Data Protection?*, Cham-Heidelberg-New York-Dordrecht-Londra, Springer, 2009, p. 27.

Da un punto di vista contenutistico, invece, le linee guida dell'OECD e la Convenzione n. 108 hanno avuto come principale il merito quello di aver definito alcuni punti di sintesi rispetto ai principi condivisi sulla protezione dei dati, consolidando così anche il valore essenziale di alcuni diritti che ancor oggi informano la disciplina di settore[57].

Se però si sposta l'attenzione su quanto concerne precipuamente il rapporto tra diritti e dati, è soprattutto il documento elaborato a Strasburgo a dare un contributo essenziale alla rilettura delle garanzie tradizionali, favorendo, per l'appunto, la graduale codificazione di una disciplina sui dati ispirata alla tutela dei diritti fondamentali[58]. Il testo della Cedu, infatti, non conteneva alcun riferimento esplicito alla protezione e all'uso delle informazioni personali. L'art. 8 di tale Convenzione, infatti, pur richiamando delle garanzie riconducibili al concetto di *privacy*, letteralmente, sancisce "solo" il diritto al rispetto della vita privata e familiare, circoscrivendo il suo ambito di applicazione alla tutela della sfera privata, del domicilio e della corrispondenza[59]. Inoltre, il sistema elaborato a Strasburgo si connota per avere una forte propensione pubblicistica, concentrandosi soprattutto

---

[57] Sono state infatti le Linee Guida OECD e la Convenzione n. 108 a fornite un «minimo comune denominatore» sul tema della *data protection*, soprattutto rispetto alle riflessioni sviluppate nel contesto europeo. G. TIBERI, *Riservatezza e protezione dei dati personali*, in M. CARTABIA (a cura di), i *Diritti in azione*, Bologna, Il mulino, 2007, pp. 375 ss.; L. CALIFANO, *Privacy: Affermazione e pratica di un diritto fondamentale*, Napoli, Editoriale Scientifica, 2016, p. 31

[58] A commento, di vedano: V. FROSINI, *La Convenzione Europea sulla protezione dei dati*, in *Rivista di Diritto Europeo* 24, 1984; P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione europea*, pp. 49 ss.; G. BUTTARELLI, *Banche dati e tutela della riservatezza*, cit., pp. 8 ss.; G. TIBERI, *Riservatezza e protezione dei dati personali*, cit., pp. 376-377.

Alla disciplina definita dalla Convenzione n. 108 sono poi seguite una serie di Raccomandazione da parte del Comitato dei Ministri in seno al Consiglio d'Europa. Questi documenti hanno definito meglio alcuni principi generali rispetto ad ambiti specifici come, ad esempio, il trattamento dei dati in ambito medico, nell'attività della pubblica amministrazione, per le prestazioni socio-assistenziali e previdenziali, nelle attività di indagine e di polizia, nei rapporti di lavoro, per le attività di *marketing* diretto e nel settore delle telecomunicazioni (con particolare cura soprattutto rispetto al tema delle intercettazioni telefoniche e telematiche).

[59] Convenzione EDU, art. 8, § 1.

sui rapporti tra i cittadini e lo Stato e sulle indebite ingerenze nella sfera privata da parte delle autorità pubbliche[60].

È proprio rispetto a questi punti che si evince il contributo decisivo della Convenzione n. 108. Facendo leva sui contenuti dell'art. 8 Cedu, il Consiglio d'Europea focalizza il suo intervento sul rispetto della vita privata in relazione al trattamento automatizzato dei dati personali[61], proponendo così una serie di soluzioni minimali ad alcune questioni essenziali.

Così facendo, viene dato definitivamente spazio ad alcuni contenuti fondamentali sulla qualità dei dati, primi tra tutti i principi di finalità e di legalità[62]. Emerge poi una più chiara consapevolezza circa i rischi di discriminazione legati al trattamento dei dati c.d. sensibili. In tal senso, vengono posti alcuni chiari limiti ad un incondizionato utilizzo di tali informazioni, soprattutto nell'ambito dei processi automatizzati[63]. Vengono poi confermati i diritti essenziali dell'interessato, con la specifica raccomandazione di renderne effettivo l'esercizio di fronte all'autorità giudiziaria[64]. In questo modo, a fianco dei riferimenti tradizionali – come, ad esempio, il diritto a sapere del trattamento e di conoscere il titolare del medesimo, il potere di rettifica e aggiornamento delle informazioni erronee e la cancellazione di quelle elaborate illegalmente – si fanno strada anche alcuni accorgimenti circa i limiti di conservazione, tratteggiando così, implicitamente, i contorni del diritto all'oblio.

Invero, va peraltro rilevato come la Corte europea dei diritti dell'uomo (Corte Edu) già in altri casi si fosse orientata a favore di un'interpretazione flessibile dei contenuti dell'art. 8 Cedu, ammettendo un'estensione delle relative tutele anche ai profili informativi. Tuttavia, è soprattutto a seguito dell'adozione della Convenzione

---

[60] *Ibidem,* § 2.

[61] Consiglio d'Europa, Convenzione n. 108 del 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, art. 1.

[62] *Ibidem*, art. 5.

[63] *Ibidem*, artt. 6-7.

[64] *Ibidem*, art. 8.

n. 108 che nella giurisprudenza convenzionale cominciano a rinvenirsi riferimenti più o meno espliciti alla tutela dei dati personali, affrontando così le questioni che andavano via via emergendo con il progresso delle nuove tecnologie[65].

In particolare, nel susseguirsi delle pronunce su questi temi, la Corte ha progressivamente esteso la nozione di vita privata, spingendosi oltre la sola sfera individuale e consolidando alcuni meccanismi di controllo sull'utilizzo dei dati personali, come il diritto di accesso[66] e di rettifica[67]. Allo stesso modo, vengono valorizzati in questa sede anche alcuni principi fondamentali, come quelli di necessità, proporzionalità e finalità del trattamento[68], cominciando a delineare il ruolo delle autorità garanti come componenti essenziali del sistema di tutela[69].

In prospettiva, inoltre, pensando alla dimensione costituzionale della disciplina sui dati, rileva il fatto che, all'interno di questa cornice giuridica così rinnovata, i limiti al trattamento dei dati siano agganciati ai "parametri" indicati dal § 2 dell'art. 8 Cedu, ossia ad una valutazione di compatibilità con le condizioni necessarie allo sviluppo e alla conservazione di una società democratica.

Tuttavia, non si possono sottacere alcuni evidenti lacune dell'impostazione sviluppata in seno al sistema di Strasburgo.

In primo luogo, guardando alle caratteristiche specifiche dell'atto-fonte, la Convenzione n. 108, pur avendo "costituzionalizzato" a livello europeo alcuni

---

[65] Corte EDU, *Malone c. Regno Unito*, sent. 2 agosto 1984, n. 8691/79, § 84; *Copland c. Regno Unito*, sent. 3 aprile 2007, n. 62617/00, § 43; *Amann c. Svizzera*, sent. 16 febbraio 2000, n. 27798/95, § 65*; Rotaru c. Romania*, sent. 4 maggio 2000, n. 28341/95, §§42-43*; P.G. e J.H. c. Regno Unito*, sent. 25 settembre 2001, n. 44787/98, § 57.

[66] Corte EDU, *Gaskin c. Regno Unito*, sent. 7 luglio 1989, n. 10454/83; *Antony e Margaret McMichael c. Regno Unito*, sent. 24 febbraio 1995, n. 16424/90; *Guerra c. Italia*, sent. 19 febbraio 1998, n. 14967/89; *McGinley & Egan c. Regno Unito*, sent. 28 gennaio 2000, nn. 21825/93 e 23424/94.

[67] Corte EDU, *Rees c. Regno Unito*, sent. 25 ottobre 1986, n. 9532/81; *Cossey c. Regno Unito*, sent. 27 settembre 1990, n. 10843/84; *B. c. Francia*, sent. 25 marzo 1992, n. 13343/87; *Christine Goodwin c. Regno Unito*, sent. 11 luglio 2002, n. 28957/95.

[68] Corte EDU, *Peck c. Regno Unito*, sent. 28 gennaio 2003, n. 44647/98, § 62; *Perry c. Regno Unito*, sent. 17 luglio 2003, n. 63737/00, § 40; *P.G. e J.H. c. Regno Unito*, cit., § 59.

[69] Corte EDU, *Klass c. Germania*, sent. 6 settembre 1978, n. 5029/71, § 55; *Leander c. Svezia,* sent. 26 marzo 1987, n. 9248/81, §§ 65-67*; Rotaru c. Romania*, cit. §§ 59-60.

principi sulla protezione dei dati, ha posto più di qualche inconveniente. Trattandosi di un documento di diritto internazionale, innanzitutto, questa aveva richiesto di essere attuata mediante un atto di recepimento interno: un adempimento cui molti Stati, tra cui l'Italia, si sono dimostrati alquanto insofferenti[70]. A ciò si aggiungono poi delle ulteriori criticità, legate ora alla completa deregolamentazione dei trasferimenti di dati verso Paesi terzi non contraenti, ora alla mancata previsione di meccanismi di garanzia minimi come il necessario consenso dell'interessato[71].

In secondo luogo, considerando invece l'impostazione del documento rispetto ai contenuti, la giurisprudenza della Corte Edu, pur riconoscendo il valore normativo della Convezione, ha continuato a rifarsi soprattutto allo schema proposto dall'art. 8 Cedu, limitando così i propri interventi alle indebite ingerenze e all'illecito utilizzo dei dati personali nei rapporti tra i cittadini e le autorità pubbliche, lasciando invece nel limbo le questioni relative ai rapporti tra i privati.

Alla luce di queste considerazioni, dunque, il quadro che si evince mette in luce essenzialmente due aspetti. Da un lato, la Convenzione n. 108 e dalla giurisprudenza di Strasburgo – come già ricordato – hanno contribuito ad emancipare la protezione dei dati personali dalla sua originaria vocazione tecnico-procedurale per attrarla nell'ambito del dibattito sui diritti fondamentali. A quest'orientamento faranno seguito non solo gli Stati che, a partire dagli anni Ottanta, cominceranno a dotarsi di nuove leggi sulla protezione dei dati personali, ma anche la stessa Comunità europea nel formulare la propria disciplina. Dall'altro, i limiti riscontrati in questa disciplina e nelle sue successive interpretazioni contribuiranno ad incoraggiare un approccio più energico rispetto alla regolamentazione di queste attività, introducendo specifiche garanzie costituzionali

---

[70] L'Italia, infatti, pur avendo aderito alla Convenzione il 2 febbraio 1983, ha provveduto alla sua ratifica soltanto nel 1997, dopo essersi dotata di una propria disciplina interna sulla protezione dei dati con la l. n. 675/1996.

[71] Limiti riscontrati, *ex multis*, in P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione europea*, pp. 62; G. BUTTARELLI, *Banche dati e tutela della riservatezza*, cit., pp. 26 ss.;

rispetto alla tutela delle informazioni fino ad arrivare all'elaborazione di una normativa più trasversale e omnicomprensiva a livello comunitario.

### *2.3. La protezione dei dati personali nel diritto costituzionale di alcuni Stati*

Esaminando le prime leggi sulla protezione dei dati e i loro lavori preparatori, la dottrina non ha mai mancato di sottolineare le evidenti implicazioni costituzionali di questa materia. Tali normative, infatti, puntando a garantire valori essenziali – come il rispetto della vita privata nell'utilizzo delle informazioni personali, la tutela dell'autonomia e dell'autodeterminazione individuale, l'integrità e la trasparenza nei rapporti istituzionali tra i cittadini e lo Stato – sono spesso state lette come una traduzione delle garanzie proprie dello Stato di diritto in un contesto sempre più informatizzato[72].

Evidentemente, le Costituzioni approvate immediatamente nel secondo dopoguerra non avevano assimilato queste preoccupazioni e, dunque, così come per altri diritti legati allo sviluppo delle nuove tecnologie, non erano state previste particolari previsioni *ad hoc*[73].

Certo, a differenza del passato, nelle Carte di molti ordinamenti europei era stata riconosciuta qualche forma di tutela a favore della riservatezza della sfera

---

[72] L.A. BYGRAVE, *Data Protection Law – Approaching Its Rationale, Logic and Limits*, L'Aia-Londra-New York, Kluwer Law International, 2002: «At a higher level of abstraction, we can discern within data protection laws considerable influence from older doctrines on 'rule of law'» (p. 119). Su questo punto, si vedano inoltre, sempre nella stessa opera, i riferimenti relativi ai i valori meta-individuali legati alla tutela della *privacy*, come, ad esempio, la democraticità dell'ordinamento e il pluralismo (pp. [133-136]) e all'effettive garanzie approntate in tal senso dalla legislazione sui dati personali in diversi ordinamenti europei (p. 156). Dello stesso avviso, seppur in termini diversi, S. RODOTÀ, *Tecnologie e diritti*, cit., pp. 41 ss.

[73] Questo non è un caso che interessa soltanto la Costituzione italiana. In generale, in Europa, il diritto alla riservatezza aveva trovato un riconoscimento al quanto incerto nelle Carte fondamentali dei diversi Stati, tant'è che normalmente è proprio l'art. 8 Cedu a rappresentare un punto di sintesi rispetto ai diversi orientamenti; un intervento di "armonizzazione" *sui generis* che risale comunque al 1950. Cfr. A. DI MARTINO, *I profili costituzionali della privacy negli Stati Uniti e in Europa*, cit., capitolo 3.

privata, ma, anche in questo caso, i meccanismi di garanzia si sono basati soprattutto sull'interpretazione sistematica di alcuni principi fondamentali, ancorando questo nuovo diritto alla protezione della dignità umana e al libero sviluppo della personalità[74].

Le Costituzioni di c.d. ultima generazione, tuttavia, hanno visto la luce in un periodo in cui era già maturata una nuova consapevolezza rispetto a questi temi e, venendo questi Stati dall'esperienza di regimi autoritari, spesso si sono mostrati più attenti[75]. In questa prospettiva, dunque, nell'ottica di approfondire come il diritto costituzionale europeo abbia affrontato le questioni inerenti il complicato rapporto tra diritti e informazioni, è opportuno analizzare qualche caso specifico.

In Portogallo, ad esempio, con la Carta del 1976, per la prima volta alcuni principi sulla protezione dei dati personali entrano a far parte di una Costituzione nazionale. L'art. 35, infatti, in ben sette commi, sancisce alcune particolari garanzie relative all' «uso delle tecnologie dell'informazione». Scorrendo i diversi punti, si osserva come, in questo caso, l'Assemblea costituente abbia scelto di elevare al rango di diritti costituzionali elementi essenziali della disciplina sui dati, includendo i diritti di accesso, rettifica e aggiornamento. A queste garanzie si sono aggiunti

---

[74] Ad esempio, nel diritto di area tedesca, sebbene si fosse ragionato molto sui presupposti alla tutela della sfera privata nell'ambito delle teorie relative ai diritti della personalità, l'effettivo riconoscimento costituzionale di un simile diritto risale soltanto al 1949. Con l'entrata in vigore della nuova legge fondamentale, infatti, facendo leva proprio sul principio di dignità umana e al diritto ad un libero sviluppo della personalità (artt. 1, comma 2 e 2, comma 1 LF) viene riconosciuto embrionalmente un diritto alla tutela della sfera privata, come derivazione sistematica e indiretta di tali principi costituzionali. Allo stesso modo, in Francia, una tutela sistematica della *vie privée* a livello costituzionale interviene soltanto ad opera della giurisprudenza, a partire dagli anni Settanta. Cfr. A. DI MARTINO, *I profili costituzionali della privacy negli Stati Uniti e in Europa*, cit., rispettivamente, pp. 132 ss. (Germania); pp. 202 ss. (Francia).

[75] I principali riferimenti bibliografici per questa parte consistono in G. GONZÁLEZ FUSTER, *The emergence of data protection as a fundamental right of EU*, cit.. pp. 66 ss.; L.A. BYGRAVE, *Data Protection Law – Approaching Its Rationale, Logic and Limits*, cit., p. 117; F. DONATI, *Articolo 8 – La protezione dei dati di carattere personale*, in R. BIFULCO, M. CARTABIA, A. CELOTTO (a cura di), *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione europea*, Bologna, Il Mulino, 2001, pp. 83 ss.

principi e limiti, soprattutto per l'utilizzo dei dati sensibili (comma 3) [76]. Congiuntamente, e con un approccio non dissimile da quello che aveva adottato il legislatore francese, vengono introdotte ulteriori garanzie per l'accesso e l'utilizzo delle banche dati e dei *network* pubblici, delegando al legislatore la definizione della disciplina di dettaglio.

Analogamente è accaduto in Spagna, in cui, nei lavori preparatori alla carta fondamentale poi approvata nel 1978, si è ipotizzato di definire con legge ordinaria limiti e obblighi rispetto all'utilizzo dell'informatica; una serie di preoccupazioni e obiettivi poi confluiti nel disposto di cui all'art. 18 della Carta. Nonostante alcune incertezze terminologiche, infatti, nell'ultimo paragrafo della norma, dopo le tutele a favore della *intimidad personal y familiar* e delle comunicazioni e del domicilio, vi è questa delega al legislatore ordinario a che provveda per il settore delle nuove tecnologie[77].

Tra questi primi esempi, spicca poi anche l'esperienza austrica. In questo ordinamento, infatti, pur avendo adottato una legge federale di rango ordinario sulla protezione dei dati personali, i diritti dell'interessato vengono espressamente riconosciuti come diritti fondamentali, trovando così sostanza all'interno del dettato costituzionale.

Con gli anni, poi, a questi primi pionieristici tentativi hanno fatto eco anche le Costituzioni di altri Stati, come ad esempio, l'Olanda, la Svezia, la Polonia,

---

[76] In particolare si prevede un divieto nei seguenti termini: (3) Information technology may not be used to treat data concerning philosophical or political convictions, party or trade union affiliations, religious faith, private life or ethnic origins, save with the express consent of the data subject, or with an authorization provided for by law and with guarantees of non-discrimination, or for the purpose of processing statistical data that are not individually identifiable.

[77] Proprio perché la Costituzione prevede che il legislatore statale provveda rispetto a questi temi, la dir. 46/95, così come il nuovo reg. 679/2016 sono stati assimilati con una legge nazionale, recependo così con un atto di diritto interno i principi e la disciplina di matrice comunitaria. Cfr. M. RUBECHI, *La transizione verso il nuovo sistema delle fonti europee di protezione dei dati personali*, in L. CALIFANO, C. COLAPIETRA (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2017, pp. 391-392.

l'Ungheria e la Slovacchia, tanto da far suggerire a qualcuno l'opportunità di emulare analoghe iniziative con degli emendamenti specifici anche della nostra Carta fondamentale[78].

Un contributo particolarmente significativo nell'evoluzione di questi orientamenti proviene però dal fondamentale apporto della giurisprudenza costituzionale tedesca, che in una pronuncia del 1983, decidendo della legittimità della normativa sul censimento, è arrivata a sancire uno specifico diritto alla c.d. «autodeterminazione informativa»[79].

Di per sé, un simile concetto si era già fatto strada sotto altre vesti; non era infatti la prima volta che si guardava alla protezione dei dati personali come ad un diritto di controllo sui contenuti riferibili a sé stessi. Tuttavia, la peculiarità delle conclusioni elaborate dalla Corte federale sta nel fatto di riconoscere nella c.d. *informationelle Selbstbestimmung* un nuovo diritto fondamentale della personalità, specifico e concettualmente autonomo rispetto ad altre figure.

Guardando al percorso descritto finora, molti hanno visto in questa pronuncia l'espressione della più autentica vocazione del diritto costituzionale, chiamato ad espandere la portata dei valori racchiusi nel testo della Legge fondamentale in funzione delle sfide poste dallo sviluppo tecnologico e sociale, anche laddove non vi sia una specifica norma[80].

---

[78] G.M. SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in R. NANIA, P. RIDOLA (a cura di), *I diritti costituzionali*, Torino, Giappichelli, 2006, in cui si legge come «questi esempi inducono a ritenere opportuno, se non addirittura necessario, un aggiornamento del nostro testo costituzionale in ordine ad una questione ormai cruciale ai fini dell'effettiva garanzia di quel libero svolgimento della personalità che è alla base dei diritti involabili dell'uomo» (p. 628). Dello stesso avviso, S. RODOTÀ, *Il mondo nella rete. Quali diritti, quali vincoli*, Roma, Laterza, 2014, p. 16.

[79] Si tratta della famosa *Volkszählungsurteil* (la sentenza sul censimento) del 1983 (BVerfGE (65) 1983). Testo consultabile nella traduzione inglese a questo link.

[80] M. ALBERS, *Realizing the Complexity of Data Protection*, in S. GUTWIRTH, R. LEENES, P. DE HERT (a cura di), *Reloading data protection. Multidisciplinary Insights and Contemporary Challenges*, Dordrecht-Londra- Heidelberg-New York, Springer, 2014, p. 218.

Tra le righe, leggendo la sentenza, si coglie in questo caso come i giudici si siano fatti interpreti, prima ancora che delle norme, delle preoccupazioni che si erano condensate attorno agli usi e agli abusi dei dati personali. Osserva la Corte,

> La libertà delle persone di fare programmi e prendere decisioni in virtù delle loro prerogative di autodeterminazione può essere significativamente inibita se queste non sono in grado di determinare con un sufficiente grado di certezza quali delle informazioni che li riguardano possono essere divulgate in certi ambiti della loro sfera sociale e così, in qualche misura, ciò di cui possono disporre i loro possibili interlocutori[81].

Come si evince anche in queste parole, è chiaro come, fin da principio, la protezione dei dati personali, nel contesto europeo, non possa essere letta come una serie di misure volte alla difesa della sola sfera privata. Come rivelano le osservazione dei giuridici tedeschi, si tratterebbe piuttosto di un'aspettativa di tutela più generalizzata e dinamica, volta a garantire gli interessi dell'individuo in tutti i profili della vita di relazione in cui, in qualche modo, siano presenti particolari risvolti informativi. In altre parole, l'autodeterminazione informativa, costituisce un nuovo potere del singolo che gli consente di decidere autonomamente sulla rivelazione e sull'utilizzo dei propri dati[82]. E rispetto alla precedente tradizione normativa in materia di protezione dati, questo nuovo diritto fondamentale è da intendersi non tanto come una singola posizione giuridica soggettiva, quanto piuttosto come un «fascio di diritti e obblighi che nascono dall'intreccio della norma costituzionale con la sua attuazione legislativa»[83].

A conclusione di queste brevi premesse sugli antecedenti storico-culturali che hanno guidato lo sviluppo della disciplina e del diritto alla protezione dei dati

---

[81] BVerfGE (65) 1983, § 2, pt. 1.a). Traduzione non ufficiale. Ogni riferimento può essere comparato con il testo originale o con la versione inglese che qui si riporta: «The freedom of individuals to make plans or decisions in reliance on their personal powers of self-determination may be significantly inhibited if they cannot with sufficient certainty determine what information on them is known in certain areas of their social sphere and in some measure appraise the extent of knowledge in the possession of possible interlocutors».

[82] *Ibidem, considerato* n. 1.

[83] A. DI MARTINO, *I profili costituzionali della privacy negli Stati Uniti e in Europa*, cit., p. 159.

personali in diversi Stati europei, si può osservare come, fin da principio, in questa normativa vengano ad affermarsi una serie di *nuovi diritti*, che dialogano con i valori tutelati da altri diritti e libertà fondamentali andando oltre la sola sfera privata. La tecnica adottata dai costituenti che su questi temi si sono cimentati, inoltre, dimostra come una volta affermati i principi, questi necessitino inevitabilmente dell'intervento del legislatore, creando così una profonda unione tra il diritto costituzionalmente tutelato e la sua attuazione attraverso la legge ordinaria.

Alla luce di queste considerazioni, dunque, vi sono utili spunti di riflessione per esaminare il percorso che ha portato alla positivizzazione della disciplina sulla protezione dei dati in Italia; tema che sarà sviluppato nei prossimi paragrafi soffermandosi prima sull'evoluzione della giurisprudenza costituzionale e, poi, sugli sviluppi del complesso normativo che gravita attorno al Codice Privacy.

### 3. Il percorso della giurisprudenza costituzionale italiana verso la protezione dei dati personali

Per capire come si sia sviluppata la disciplina sulla protezione dei dati nel contesto italiano è necessario partire da un attento studio della giurisprudenza.

Contrariamente a quanto accaduto in altri ordinamenti, infatti, il nostro legislatore è arrivato ad occuparsi di questi temi solo in tempi relativamente recenti, a partire dal 1996. Tuttavia, considerata la portata dei problemi accennati poc'anzi, prima di allora, le lacune della precedente normativa sono state colmate dall'intervento dei giudici comuni, della Cassazione e, non ultima, della Corte costituzionale.

Partendo dunque da un attento studio della giurisprudenza che, in qualche modo, ha affrontato il rapporto tra diritti e dati nel contesto interno, in queste pagine ci si concentrerà soprattutto sulle pronunce di quest'ultima, esaminando

come, a partire dalle riflessioni relative ai fondamenti costituzionali del diritto alla riservatezza e all'identità individuale, si possano cogliere delle indicazioni circa la copertura costituzionale del diritto alla protezione dei dati personali.

Lungo questo percorso, in particolare, si presterà attenzione ad alcuni profili specifici. Da un lato, si guarderà a come i giudici della Consulta abbiano definito il diritto alla riservatezza e all'identità personale rispetto all'utilizzo di contenuti che possono essere qualificati come dati personali. Dall'altro, invece, si esaminerà come nelle diverse pronunce vengono affrontate le questioni relative alla "sfida tecnologica", rinnovando le garanzie tradizionali ereditate dalla Carta di fronte allo sviluppo delle ICT.

### *3.1. Il diritto alla riservatezza*

Il punto di partenza, come accennato, non può che essere il diritto alla riservatezza. Mancando una puntuale previsione nel testo costituzionale, nel nostro ordinamento, il concetto di *privacy*, così come inteso in altre tradizioni giuridiche, infatti, per molto tempo è rimasto estraneo al diritto interno, tant'è che, in questo caso, a tutti gli effetti, ci si trova di fronte ad un «nuovo diritto», elaborato dalla giurisprudenza sulla trama dell'esperienza maturata in altri contesti.

Le questioni legate alla tutela della sfera privata, certo, non erano rimaste estranee al dibattito che aveva accompagnato i lavori dell'Assemblea costituente. Tuttavia, all'epoca, così come è stato per la formulazione di altre norme sui diritti, si preferì una soluzione più tradizionalista, dando spazio nella Carta solo alla disciplina di quelle figure giuridiche tradizionalmente consolidate[84].

[84] Sebbene infatti le questioni legate allo sviluppo delle tecnologie e al loro impatto sui diritti delle persone fossero stati messi ampiamente a tema nella giurisprudenza straniera e il dibattito su questi temi non fosse per nulla estraneo ai

Il problemi legati al tema della *privacy*, dunque, a tutta prima sono emersi come espressione dello sviluppo sociale: questioni per lo più rivolte ai giudici comuni, chiamati a pronunciarsi soprattutto sui limiti del diritto di cronaca[85]. È a partire dagli anni Cinquanta, infatti, che comincia ad emergere una chiara consapevolezza del fatto che, per come si stavano evolvendo i mezzi di comunicazione e informazione, sarebbe stato presto necessario garantire tutela non solo alla privatezza del domicilio fisico, ma anche quella della dimora «ideale». L'obiettivo che ci si prefiggeva era quello di assicurare un diritto «alla libera autodeterminazione nello svolgimento della personalità»[86], volto essenzialmente ad elevare come una sorta di limite implicito alla libertà di espressione a tutela della persona che, in qualche modo, potesse esserne oggetto[87].

---

Costituenti, così come in altri casi, in tema di diritti fondamentali, si preferì concentrare l'attenzione su altri aspetti, legati ad una visione più tradizionale (come insegna la formulazione dell'art. 21 Cost. in cui i riferimenti puntuali sono riservati solo alla disciplina sulla stampa). Cfr. A. BARBERA, *Principi fondamentali. Articolo 2*, in G. BRANCA (a cura di), *Commentario alla Costituzione*, Bologna-Roma, Zanichelli, 1975, p. [53-55].

[85] Rispetto alla giurisprudenza di questo periodo si ricordano soprattutto i casi che avevano coinvolto personaggi pubblici come Enrico Caruso (C. Cass., 22 dicembre 1956, n. 4487) Claretta Petacci (C. Cass., 20 aprile 1963, 990) e la regina dell'Iran Soraya Esfandiari (C. Cass., 27 maggio 1975, n. 2129).

[86] C. Cass., sent. 20 aprile 1963, n. 990, in cui si legge che «il fondamento in diritto positivo di un diritto assoluto di personalità può ravvisarsi nell'art. 2 Cost., il quale (…) ammette con ciò un diritto di libera autodeterminazione nello svolgimento della personalità nei limiti della solidarietà considerati».

[87] G. GIAMPICCOLO, *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, in *Rivista trimestrale di diritto e procedura civile*, 1958; A. DE CUPIS, *Teoria generale, diritto alla vita e all'integrità fisica, diritto sulle parti staccate del corso e sul cadavere, diritto alla libertà, diritto all'onore e alla riservatezza*, Milano, Giuffrè, 1958; ID., *I diritti della personalità*, Milano, Giuffrè, 1973; S. NIGER, *Le nuove dimensione della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, Cedam, 2006, pp. [39-46]; F. BILOTTA, *L'emersione del diritto alla privacy*, in A. Clemente, *Privacy*, Padova, Cedam, 1999, pp. [31-33].

Sulla scorta di queste considerazioni, si è quindi cominciato ad attingere dai principi costituzionali per definire i tratti di una nuova figura giuridica, e i primi a cimentarsi in quest'opera di "costituzionalizzazione" della riservatezza sono stati soprattutto i giusprivatisti[88]. Sfruttando il potenziale espansivo degli artt. 2 e 3 Cost. si intuiva infatti come si potessero già porre delle solide basi per garantire copertura costituzionale ai valori della *privacy* e dell'identità personale, ancorando queste nuove garanzie soprattutto al principio di libertà individuale consacrato dall'art. 13 Cost.

Pur argomentando in tal senso, tuttavia, preme rilevare come, pur rifacendosi agli ideali americani del *right to privacy*, questi diritti nell'ordinamento italiano non possano vantare la medesima copertura. La Corte di cassazione, infatti, anche quando ha avuto l'occasione di definire il contenuto di tale figura nel contesto nazionale, inizialmente, si è concentrata sulla dimensione negativo-difensiva di tale diritto, enfatizzando soprattutto la sua attitudine ad essere intesa come una «tutela di quelle situazioni e vicende strettamente personali e familiari, le quali, anche se verificatesi fuori dal domicilio domestico, non hanno per terzi un interesse socialmente apprezzabile»[89].

Se queste sono le basi su cui dapprima si è concentrata la giurisprudenza di legittimità, sul fronte del diritto costituzionale il tema ha avuto significativi sviluppi soprattutto grazie ai successivi interventi del Giudice delle leggi. Il diritto della

---

[88] Circa la c.d. «costituzionalizzazione del diritto privato», si vedano, *ex multis*, A. CERRI, *La costituzione e il diritto privato*, in P. RESCIGNO (dir.), *Trattato di diritto privato*, v. I., Torino, Utet, 1999, pp. 127 ss.; G. GAMBARO, R. PARDOLESI, *L'influenza dei valori costituzionali sul diritto civile*, in A. PIZZORUSSO, V. VARANO (a cura di), *L'influenza dei valori costituzionali sui sistemi giuridici contemporanei*, Milano, Giuffrè, 1985, pp. 5 ss.

[89] Il passaggio citato, tratto dalla sentenza 17 maggio 1975, n. 2129, allude al caso *Esfandiari*, in cui la Suprema Corte, trovandosi a decidere circa il bilanciamento tra tutela della vita privata di un personaggio pubblico (nella fattispecie concreta, la già regina di Persia, Soraya Esfandiari) e la libertà di cronaca, aveva per la prima volta utilizzato, nello specifico, l'espressione *privacy*, pur circoscrivendola – come si evince – alla sola riservatezza.

riservatezza, infatti, è passato più volte al vaglio della giurisprudenza costituzionale, pur seguendo un percorso tutt'altro che lineare e spesso intervallato negli anni da «lunghe pause di riflessione»[90].

Inizialmente, infatti, la dottrina in questo settore aveva mostrato non poche resistenze al riconoscimento di un diritto costituzionale alla riservatezza[91], in quanto, guardando alle solide garanzie previste dalla Carta a favore della libertà di manifestazione del pensiero, si temeva che una simile figura giuridica avrebbe potuto costituire un limite eccessivo al diritto sancito dall'art. 21 Cost.

In un primo momento, dunque, ritenendo esistessero comunque valide alternative per assicurare ugualmente la tutela della dimensione privata, si è preferito *bypassare* questo tema, ritenendo che eventualmente di questi problemi avrebbe potuto ben occuparsene il legislatore ordinario[92].

Tuttavia, a distanza di vent'anni da queste iniziali chiusure, la Corte costituzionale si è vista sempre più coinvolta in questi problemi, e ha quindi colto l'occasione per inaugurare una propria serie giurisprudenziale sul tema della *privacy,*

---

[90] E. FRONTONI, *La giurisprudenza costituzionale*, in A. CLEMENTE (a cura di), *Privacy*, cit., p. 65.

[91] In quello che Augusti Cerri non ha esitato definire come una «diffidente prudenza» (in ID., *Riservatezza*, in *Enciclopedia giuridica*, v. XXVII, Istituto della Enciclopedia Italiana, Roma, 1995, p. 2).

[92] In particolare, gli argomenti che si erano opposti alla possibilità di riconoscere tutela costituzionale al diritto alla riservatezza possono essere riassunte in due tesi. Da un lato vi erano quanti sostenevano che la lesione di tale diritto non raggiungesse le soglie di offensività minime da pregiudicare l'integrità e la dignità della persona tanto da renderlo un diritto costituzionale (di questa scuola, *ex multis*, S. FOIS, *Principi costituzionali e libertà di manifestazione del pensiero*, Milano, Giuffrè, 1957, pp. 227-228) mentre dall'altro vi erano quelli che ritenevano che, pur non essendo un diritto costituzionale a sé, potesse comunque trovare adeguate tutele nelle fonti di rango ordinario (*ex multis,* C. ESPOSITO, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, in *Rivista italiana di scienze giuridiche*, 1957-1958, n. 89, pp., 86-87).

contribuendo ad un primo riconoscimento di questo nuovo diritto nel nostro ordinamento.

Le pronunce di legittimità avevano già evidenziato come le questioni più critiche fossero quelle legate al bilanciamento tra la tutela dell'intimità e della privatezza e l'esercizio della libertà di stampa, e questo è risultato particolarmente stringente soprattutto nei casi in cui ci si era trovati a discutere sulle condizioni di utilizzo delle immagini della persona interessata e dei suoi prossimi congiunti.

In ragion di ciò giudici costituzionali, per prima cosa hanno chiarito come alcuni diritti di libertà affermati nella prima parte della Costituzione debbano essere ricondotti ai diritti inviolabili dell'uomo sanciti dall'art. 2 Cost, tracciando una sorta di collegamento specie-genere. Rispetto agli interessi tutelati, quindi, il singolo non vanta una pretesa soltanto nei confronti dei pubblici poteri, bensì un'aspettativa *erga omnes*[93], in grado di estendersi anche sul piano dei rapporti orizzontali con altri privati.

Sulla base di queste premesse, la Corte nel tempo ha quindi argomentato a favore del riconoscimento di una serie di figure inedite, spaziando dalla riservatezza della propria immagine[94] al riserbo sulle proprie convinzioni personali, fino alla segretezza di conversazioni e dialoghi telefonici, individuando astrattamente dei limiti sostanziali all'esercizio di altri diritti fondamentali[95]. Allo stesso modo, alla luce

---

[93] Corte Cost, sent. 122/1970, *considerato in diritto*, § 2.

[94] Sempre con riferimento alla sent. n. 122/1970, così nel commento di M. MAZZOTTI DI CELSO, *Diritto all'immagine e Costituzione* in *Giurisprudenza civile,* 1970, 1533, in cui, appunto si allude al diritto «alla riservatezza dell'immagine stessa».

[95] I riferimenti sono, rispettivamente, alle sentenze sulle questue (Corte Cost, sent. 12/1972) e sul rapporto tra l'art. 15 Cost. e la disciplina sulle intercettazioni telefoniche (Corte Cost, sent. n. 38/1973). In queste prime pronunce, tuttavia, pur enucleando i contenuti minimi della riservatezza deducendoli come dimensione negativa di altri diritti previsti dalla Carta (A. CERRI, *Libertà negativa di manifestazione del pensiero e di comunicazione privata. Diritto alla riservatezza: fondamenti e limiti*, in *Giurisprudenza Costituzionale*, I, 1974, pp. 610 e 615), i giudici costituzionali non sono

di queste prime aperture a favore della privatezza, sono stati inclusi in quest'ambito anche profili inizialmente impensati, tanto da ammettere come un vero e proprio diritto l'interesse a non dover ascoltare l'opinione altrui, così come quello ad una libera formazione dei propri convincimenti (qui secondo una sensibilità molto affine alla *privacy* d'oltreoceano)[96].

È grazie a queste prime pronunce, dunque, che la Corte comincia a far emergere i fondamenti costituzionali di questo «nuovo diritto», riconducendolo ai diritti inviolabili della persona[97]. Va rilevato, inoltre, come in questa operazione, oltre agli ovvi riferimenti ai parametri in precedenza utilizzati anche nella giurisprudenza di legittimità (gli artt. 2 e 3, comma 2, e 13, comma 1, Cost.) i giudici costituzionali abbiano deciso di portare a sostegno dei loro argomenti alcuni contenuti della Cedu, legittimando così la tutela di questo diritto anche per mezzo dell'art. 8 della Convenzione[98].

### *3.2. L'assimilazione del concetto di privacy*

Quelli appena descritti sono dei segnali che documentano dei primi segni di apertura, rispetto ad una tradizione rimasta fino a quel momento per molto tempo

---

sempre arrivati a sancire un bilanciamento a favore di quest'ultimo, spesso stabilendo la prevalenza di altri interessi. (sentt. n.122/1972, 38/1973).

[96] Questo quanto è emerso in occasione della sentenza sulla disciplina limitativa della propaganda elettorale (Corte Cost, sent. n. 138/1985) in cui il concetto di riservatezza è stato utilizzato con l'intento di preservare la tranquillità interiore dell'elettore, rispetto ai messaggi lanciati lungo le strade con l'uso degli altoparlanti. Circa l'evoluzione della nozione di riservatezza, v. A. CERRI, *Diritto di non ascoltare l'altrui propaganda*, in *Giurisprudenza Costituzionale*, I, 1985. Alcuni brevi spunti per una comparazione con il diritto americano in E. FRONTONI, *La giurisprudenza costituzionale*, cit. p. 65.

[97] L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, Editoriale Scientifica, 2016, p. 18.

[98] C. Cost, sent. 122/1970, *considerato in diritto*, § 2.

inerte rispetto ai problemi legati al tema della *privacy*. Tuttavia è soltanto negli anni Novanta che nella giurisprudenza costituzionale cominciano ad aprirsi dei veri spiragli rispetto alle questioni legate alla *data protection*.

Certo, è ancora presto perché si possa parlare di un vero e proprio diritto alla protezione dei dati, tant'è che la legge che introduce esplicitamente questa disciplina nel nostro ordinamento interverrà qualche anno più tardi. Tuttavia, è in quel periodo che la Corte comincia a dimostrare la propria sensibilità nei confronti del problematico rapporto tra diritti e informazioni. E questo, come osservato[99], è accaduto anche grazie alla presenza tra i giudici della Corte di Antonio Baldassare e Cesare Mirabelli, due giuristi che in quegli stessi anni si stavano cimentando sui temi della "nuova" *privacy*, tra protezione dei dati e tutela dei diritti[100]. Quanti avevano cominciato ad occuparsi di questi temi, infatti, si erano ormai resi conto da tempo dei limiti intriseci di un approccio meramente negativo come quello promosso sul fronte della riservatezza. La diffusione dei computer e dell'informatica e, con essi, la possibilità di gestire in modo automatizzato grandi banche dati, vedeva nella raccolta delle informazioni soltanto un semplice presupposto, concentrandosi poi il momento principale dell'attività di trattamento nei successivi utilizzi dei contenuti ottenuti.

Alla luce di queste considerazioni, dunque, nella giurisprudenza costituzionale italiana per la prima volta ha cominciato a farsi strada il concetto di *privacy* – inedito per il nostro ordinamento –, inteso non solo come traduzione di "privatezza"[101] ma

---

[99] A. DI MARTINO, *I profili costituzionali della privacy negli Stati Uniti e in Europa*, cit., p. 170.

[100] A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, Roma, Bulzoni Editore, 1975; C. MIRABELLI, *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *Diritto dell'informatica e dell'informazione*, 1993.

[101] C. Cass, sentenza 17 maggio 1975, n. 2129. Un orientamento che, come già visto anche rispetto alla precedente giurisprudenza costituzionale, si era ormai consolidato come sinonimo di riservatezza.

come insieme di principi atti a garantire il «diritto al controllo sulle proprie informazioni»[102].

Questo semplice inciso, invero, racchiude in sé un tassello molto importante del percorso che ha portato all'elaborazione di un nuovo diritto sui dati. La Corte, infatti, ha constatato innanzitutto come questo genere di garanzie costituisca una tradizione ormai consolidata «in tutti gli ordinamenti giuridici delle nazioni più civili». E già allora è emerso in modo chiaro come l'obiettivo di queste tutele sia quello di evitare che, a causa di un incauto trattamento dei dati personali, possano essere «messi in pericolo beni individuali strettamente connessi al godimento di libertà costituzionali e addirittura diritti inviolabili»[103].

La nuova *privacy*, dunque, in questa prima lettura verrebbe a configurarsi come un'etichetta cui vengono ricondotte congiuntamente la sicurezza e la riservatezza dei dati[104], facendone un «diritto strettamente strumentale»[105] perché altri interessi possano essere pienamente tutelati.

Pur incontrando qualche incertezza terminologica, questi orientamenti nel tempo hanno trovato ulteriori conferme nelle pronunce in cui la Corte ha continuato a ragionare sul rapporto tra riservatezza, libertà e segretezza (art. 15 Cost.)[106]. In più occasioni, infatti, si è chiarito come la Costituzione riconosca «un

---

[102] Corte Cost, sent. n. 139/1990, sulla disciplina del sistema statistico nazionale e i margini di autonomia regionale rispetto alle loro rispetti competenze in materia. E. FRONTONI, *Giurisprudenza costituzionale*, cit., p. 67.

[103] Corte Cost, sent. 139/1990, *considerato in diritto*, § 11.

[104] L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, cit., pp. 19-20.

[105] F. MODUGNO, *I nuovi diritti nella giurisprudenza costituzionale*, Torino, Giappichelli, 1995, p. 25.

[106] Si tratta, in particolare, si una serie giurisprudenziale che si è interessata, da un lato, della disciplina sulle intercettazioni telefoniche e l'utilizzo come prova dei dati esterni alle comunicazioni con quanto previsto dall'art. 15 Cost. (Corte Cost, sent. 366/1991; sent. n. 81/1993) e, dall'altro, delle questioni relative all'utilizzo di

particolare pregio all'intangibilità della sfera privata negli aspetti più significativi e più legati alla vita intima della persona umana», intendendola come una particolare espressione del principio di dignità[107]. Pertanto, la Consulta ha ribadito «la stretta attinenza di tale diritto al nucleo essenziale dei valori di personalità», tanto da qualificare queste garanzie «come parte necessaria di quello spazio vitale che circonda la persona».

E sulla scia di queste considerazioni cominciando ad affiorare anche nella giurisprudenza del Giudice delle leggi i rischi legati all'impatto delle nuove tecnologie sui diritti, nonché la «formidabile capacità intrusiva»[108]di questi strumenti e i limiti della legislazione vigente[109]. Come si legge in alcune pronunce, infatti, col tempo era emerso chiaramente come l'utilizzo dei dati personali e di ogni altra informazione riconducibile al soggetto, potesse prefigurare – quanto meno in astratto – nuove occasioni di interferenza; e questo non solo nei luoghi fisici della

---

sistemi di videosorveglianza nell'ambito delle indagini penali rispetto a quanto previsto dall'art. 14 Cost. (Corte Cost, sent. n. 135/2002).

[107] Corte Cost, sent. 366/1991, *considerato in diritto*, § 3.

[108] *Ibidem*.

[109] Corte Cost, sent. 135/2002, *considerato in diritto*, § 1, circa la mancata estensione delle garanzie sulle intercettazione anche alla riprese visive e alle videoregistrazioni.

quotidianità ma anche nella «proiezione spaziale della persona»[110], contribuendo a tracciare profili sempre più puntuali e dettagliati[111].

Ha cominciato così a farsi strada l'idea che ricorrendo a queste nuove tecniche si stia andando incontro ad un vero e proprio "salto qualitativo"[112] rispetto al potenziale intrusivo tipico dei sistemi precedenti, tanto da avvertire come sempre più necessario un puntuale aggiornamento del quadro delle garanzie (soprattutto in ambito penale).

In tal senso, dunque, la giurisprudenza successiva ha provveduto a chiare che, laddove il conseguimento di alcune informazioni sia imposto in termini inderogabili, il concetto di riservatezza non si limita soltanto alla tutela della sfera privata. La garanzia si amplia e si estende anche e soprattutto a protezione delle categorie di persone che, a motivo del trattamento dei loro dati, potrebbero trovarsi oggetto di

---

[110] *Ibidem*, § 2.1. Le considerazioni in esame, nello specifico, si rifanno ai presupposti che permettono di qualificare la tutela del domicilio (art. 14 Cost.) come diritto inviolabile. Gli argomenti utilizzati dalla Corte in parte considerazioni, in particolare, sono state fatte rispetto alla tutela del domicilio *ex* art. 14 Cost, assimilandole a quanto previsto a favore della riservatezza della corrispondenza (art. 15 Cost.) già riconosciuto come diritto inviolabile. «Il domicilio viene cioè in rilievo, nel panorama dei diritti fondamentali di libertà, come proiezione spaziale della persona, nella prospettiva di preservare da interferenze esterne comportamenti tenuti in un determinato ambiente: prospettiva che vale, per altro verso, ad accomunare la libertà in parola a quella di comunicazione (art. 15 Cost.), quali espressioni salienti di un più ampio diritto alla riservatezza».

[111] Come si osserva infatti sia nella sent. n. 81/1993 sia nella successiva n. 135/2002, tanto nell'ipotesi in cui si intenda produrre in giudizio come prova i dati esterni di una comunicazione telefonica, quanto nel caso in cui si predisponga un sistema di videosorveglianza da remoto, a cambiare non è l'essenza delle forme di perquisizione e indagine ammessi a livello costituzionale (ispezioni, perquisizioni, sequestri e, *latu senso*, intercettazioni) ma la natura del mezzo utilizzato per eseguirle. Collezionando più informazioni, infatti, questi si prestano ad aver una maggior valenza dimostrativa rispetto alla vita del soggetto interessato.

[112] Corte Cost, sent. n. 135/2002, *considerato in diritto*, § 2.1.

emarginazione e stigma sociale[113], imponendo così specifici accorgimenti volti a garantire una maggior confidenzialità dei dati sensibili[114] e derogando al principio di pubblicità e trasparenza quando ciò sia volto ad una maggior tutela dei soggetti più deboli[115].

Analizzando questo cambio di passo nel modo di intendere il rapporto tra diritti e dati, si possono mettere in luce almeno tre punti decisivi per il futuro del diritto alla protezione dei dati.

---

[113] Paradigmatico, in tal senso, il passaggio della sent. n. 218/1994, in cui la Corte, dichiarando incostituzionale l'assenza di un obbligo a sottoporsi ai test di accertamento sul contagio da HIV per gli operatori sanitari, constatava comunque come, sebbene tali esami fossero da ritenersi necessari per fini di interesse generale, allo stesso tempo la loro somministrazione non avrebbe potuto prescindere dalla salvaguardi della «dignità della persona, che comprendeva anche il diritto alla riservatezza sul proprio stato di salute e al mantenimento della vita lavorative e di relazione compatibile con tale stato» (*ivi*, *considerato in diritto*, § 2). Si tratta di una considerazione di particolare evidenza e di più ampio respiro, già emersa in occasione della discussione che ha accompagnato l'approvazione del c.d. Statuto dei lavoratori (legge n. 300/1970). Nel contesto italiano, quella fu la prima occasione in cui vennero introdotte delle norme per limitare l'uso di impianti audiovisivi e di altre apparecchiature con finalità di controllo sull'attività dei lavoratori (artt. 4, 5 e 6), nonché il «il divieto per il datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché sui fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore» (art. 8). Come ricorda Stefano Rodotà, «quest'ultima norma non è importante solo per la specifica disciplina introdotta, ma soprattutto perché consente di individuare nella nostra legislazione […] un tentativo di classificazione delle informazioni diverso da quelli finora correnti e introduce un divieto capace di dar vita una di quelle forme di tutela preventiva» (ID., *Elaboratori elettronici e controllo sociale*, cit., pp. 62-63)

[114] Corte Cost, sent. n. 218/1994; v. altresì sentt. nn. 257/1996; 238/1996 (tutte sentenze relative alle questioni inerenti gli accertamenti sanitari obbligatori).

[115] Corte Cost, sentt. n. 373/1992; 235/1993; ord. n. 37/1995 sulla possibilità di riconoscere una deroga al principio di pubblicità del dibattimento in alcuni riti speciali o comunque camerali a motivo della celerità del procedimento e della tutela della riservatezza e della dignità della parte. Diversamente, invece, nella non procedibilità a querela dei reati contro la libertà sessuale se connessi ad altri reati procedibili d'ufficio: Corte Cost, sent. n. 64/1998.

Innanzitutto, dopo aver introdotto una nozione ampia di *privacy*, includendovi sia i profili inerenti la riservatezza sia la protezione dei dati, la Corte costituzionale si è orientata verso un'interpretazione ibrida di questo concetto, privilegiando ora gli aspetti più legati all'autonomia e alla tutela della sfera privata *tout court*, ora concentrandosi di più sui punti critici legati alla gestione delle informazioni personali.

In secondo luogo, dopo aver preliminarmente chiarito che la riservatezza, come valore, rispetto a quanto previsto dalla Carta fondamentale, si presta a ricevere una tutela *erga omnes*, la giurisprudenza successiva si è concentrata soprattutto sui contenuti di valore, ammettendo dunque la deroga a questi principi solo se «in ragione dell'inderogabile soddisfacimento di un interesse pubblico primario costituzionalmente rilevante» e sempre entro i limiti dello strettamente necessario[116].

Infine, registrando i possibili impatti delle nuove tecnologie sulle libertà e i diritti, la Corte, dal punto di vista metodologico, si sofferma sul potenziale espansivo delle previsioni costituzionali, attingendo all'esperienza giuridica straniera e richiamandosi alle norme e ai precedenti sviluppati in sede europea, aprendo il diritto ad un riconoscimento costituzionale di una più ampia nozione di *privacy*.

### *3.3. (segue) e i suoi successivi sviluppi*

In seguito a questi essenziali chiarimenti, tuttavia, per un lungo periodo, gli interventi della Corte costituzionale in tema di *privacy* sembrano essersi limitati.

Questo fatto è stato letto da alcuni come il riflesso di una più generale tendenza verso un complessivo ridimensionamento delle decisioni in materia di

---

[116] Corte Cost, sentenza 23 luglio 1991, n. 366, *considerato in diritto*, § 3.

diritti[117]. Peraltro, non si può trascurare il fatto che, proprio in quegli anni, la legge n. 675 del 1996[118], recependo a livello nazionale la dir. CE 95/46[119], ha introdotto la prima specifica disciplina sulla protezione dei dati e la tutela della riservatezza, colmando così in qualche modo le lacune normative cui fino a quel momento la giurisprudenza costituzionale e di legittimità aveva supplito.

Cionondimeno, in seguito al consolidarsi del c.d. pacchetto *data protection*[120], la Corte costituzionale, interpellata sul tema, è tornata ad occuparsi delle questioni inerenti alla tutela della riservatezza, soffermandosi soprattutto sulle questioni inerenti la tutela dei dati personali. Questa seconda serie giurisprudenziale, rispetto alla precedente, però, presenta una radicale differenza: il Giudice delle leggi infatti è chiamato ora a pronunciarsi anche alla luce di nuovi parametri, offerti non solo dai

---

[117] A. DI MARTINO, *I profili costituzionali della privacy negli Stati Uniti e in Europa*, cit., p. 179; P.A. CAPOTOSTI, *La Corte costituzionale: giudice delle libertà o dei conflitti?,* in B. CARAVITA (a cura di), *La giustizia costituzionale in trasformazione: la Corte costituzionale tra giudice dei diritti e giudice dei conflitti*, Napoli, Jovene, 2012, pp. 227 ss. In seguito, infatti, le uniche pronunce degne di nota sono quelle relative alla tutela dei dati personali nell'ambito delle competenze regionali, come nel caso della legge della regione Marche sul "Sistema regionale di protezione civile" (Corte Cost, sentenza del 16 ottobre 2003, n. 327) e della legge della regione Emilia Romagna del 2004 sullo "Sviluppo regionale della società dell'informazione" (Corte Cost, sentenza del 23 giugno 2005, n. 271).

[118] Legge n. 675 del 31 dicembre 1996, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*. Dei contenuti di questa legge e del percorso che ha portato al suo recepimento si parlerà meglio in seguito, nel § 3.

[119] Direttiva 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.

[120] La legge n. 675/1996 è confluita nel d.lgs. 196/2003 (il c.d. Codice in materia di protezione dei dati personali). Quest'atto, come definito da alcuni un "testo unico" in materia di *privacy* (L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, cit., p. 27), contiene la disciplina che implementa nel nostro ordinamento la già citata dir. CE 45/96, e le successive dirr. CE 2002/58 e alcune disposizioni della dir. CE 2006/24 (poi dichiarata invalida dalla Corte di giustizia dell'Unione europea con la sentenza dell'8 aprile 2014, *Digital Rights Ireland*). Più approfonditamente nel capitolo 3.

riferimenti costituzionali interni, ma anche dalla disciplina delle relative direttive e – in modo particolare – dalla neo-introdotta Carta dei diritti fondamentali dell'Unione europea (CDFUE)[121].

Con riferimento a quest'ultima novità, va sottolineato fin d'ora un punto di particolare interesse. La Convenzione di Nizza, sebbene ci si fosse accordati solo per una codificazione dell'*acquis* comunitario in tema di diritti (e non per un rinnovamento del quadro delle garanzie) ha introdotto un'importante novità per quel concerne il diritto alla *privacy*. A differenza di quanto previsto in altri documenti internazionali, a livello europeo, il sistema di tutela di questo diritto prevede infatti due figure distinte: da un lato, la tutela della vita privata (art. 7 CDFUE) dall'altro, la protezione dei dati personali (art. 8, CDFUE) riconoscendo quest'ultimo come un diritto fondamentale a se stante. In qualche modo, si apre quindi una terza stagione dell'elaborazione dei fondamenti costituzionali di questi diritti, questa volta segnati più profondamente dall'innovazione tecnologica e, soprattutto, dagli esiti del processo di integrazione europea.

Sulla scorta di queste novità, a partire dagli inizi del nuovo millennio, la Corte costituzionale ha avuto quindi occasione di tornare ad occuparsi di questi temi, cimentandosi in una serie di casi focalizzati soprattutto sui profili assiologici del rapporto che lega assieme *privacy*, sicurezza e diritto di difesa[122].

---

[121] Come noto, questa Carta, proclamata a Nizza il 7 dicembre 2000, originariamente era stata concepita come una sorta di *bill of rights* europeo destinato a diventar parte integrante del progetto che avrebbe portata all'approvazione della Costituzione europea. Naufragata questa iniziativa, il documento ha avuto valore ricognitivo fino alla revisione dei Trattati del 2009, in seguito alla quale, dopo il Trattato di Lisbona, è entrata a far parte a tutti gli effetti delle fonti di rango primario *ex* art. 6 TUE.

[122] Sono gli anni immediatamente successivi all'11 settembre 2001. Sia negli Stati Uniti sia in Europa cominciano ad essere adottati dei provvedimenti straordinari per contenere le minacce del terrorismo internazionale e salvaguardare la sicurezza pubblica. In molti ordinamenti sull'onda di questa tendenza, si sono registrati dei progressivi inasprimenti delle normative di prevenzione e repressione

Nel campo delle indagini penali, infatti, avevano già allora cominciato a farsi strada nuove tecniche di intercettazione e di sorveglianza, tutte supportate dall'utilizzo delle ICT: dalla videosorveglianza da remoto alla conservazione e all'utilizzo dei metadati (la c.d. *data retention*).

I giudici delle leggi, nuovamente chiamati a chiarire dove arrivassero le garanzie costituzionali rispetto all'uso di questi nuovi strumenti, sono quindi tornati a ricordare come le libertà tutelate dalla Carta – prime tra tutte la libertà di comunicazione (art. 15 Cost.) e la libertà di domicilio (art. 14 Cost.) – siano da considerare «espressioni salienti di un più ampio diritto alla riservatezza della persona»[123] e «rientrino entrambe in una comune e più ampia prospettiva di tutela della "vita privata", tanto da essere oggetto di previsione congiunta» in numerosi documenti internazionali[124].

Va rilevato, tuttavia, come sebbene la Carta di Nizza avesse introdotto uno specifico diritto alla protezione dei dati personali, la Consulta, a sostegno di questi suoi argomenti, sembri preferire rifarsi al concetto di vita privata, assecondando così una lettura più vicina ai contenuti dell'art. 8 Cedu e dell'art. 7 CDFUE, piuttosto che alla *data protection* come intesa *ex* art. 8 CDFUE.

---

della criminalità. Per quanto riguarda la giurisprudenza costituzionale nazione i riferimenti sono alla già richiamata sentenza n. 135/2002 e alle successive nn. 372/2006, 173/2009, 20/2017. Per delle considerazioni critiche, G. DE MINICO, *Costituzione. Emergenza e terrorismo*, Napoli, Jovene, 2016, pp. 195 ss.; G. DE VERGOTTINI, *Guerra e Costituzione. Nuovi conflitti e sfide alla democrazia*, Bologna, Il Mulino, 2004, pp. 197 ss.

[123] Corte Cost, sent. n. 135/2002, *considerato in diritto*, § 2.1

[124] *Ibidem*, § 2.2. I riferimenti, nello specifico, sono all'art. 8 Cedu, all'art. 17 del Patto Internazionale per Diritti Civili e Politici (PIDCP) e, da ultimo, l'art. 7 CDFUE. Questa è la prima sentenza in cui la Corte costituzionale si rifà espressamente ai contenuti dell'art. 7 CDFUE e rappresenta, secondo alcuni, «un importante richiamo a fonti sovrannazionali che, pur essendo già stato operato in precedenza, non può che confermare l'importanza del contesto internazionale ed europeo sulla affermazione del diritto alla privacy nell'ordinamento italiano» (L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, cit. pp. 22-23)

Come dimostrano anche le pronunce successive, infatti, le questioni inerenti l'utilizzo dei dati, continuano ad essere analizzate con una lente che si concentra soprattutto sulla riservatezza delle informazioni trattate[125], lasciando in secondo piano le letture propense ad intravedere un «potere di controllare le informazioni che riguardano [un individuo] e le modalità con cui viene effettuato il loro trattamento»[126].

La Corte, dunque, così come altri Giudici europei, sembra focalizzarsi sui profili sostanziali, ossia sui valori rispetto ai quali la protezione dei dati risulta strumentale, mettendo a fuoco soprattutto i rischi legati alla tutela della riservatezza, della segretezza delle comunicazioni (art. 15 Cost.), dell'inviolabilità del domicilio (art. 14 Cost.) e del diritto di difesa (art. 24 Cost.).

Alla luce di tutto quanto detto finora, emerge chiaramente come, pur avendo assimilato il concetto, i giudici costituzionali abbiano utilizzato il termine di *privacy* per affrontare questioni legate ora alla riservatezza, ora alla protezione dei dati, ora ad entrambe, senza mai tracciare un netto distinguo tra le due figure. Certamente la giurisprudenza dimostra di aver colto l'evoluzione del sistema di tutela, e tuttavia spesso le garanzie relative alla tutela delle informazioni mancano di una propria dignità, continuando quindi ad essere sovrapposte a quelle legate alla salvaguardia della sfera privata.

### *3.4. Il diritto all'identità personale*

A compensare le lacune appena descritte, secondo alcuni, concorre un filone giurisprudenziale che si è sviluppato in parallelo a quello relativo ai temi della *privacy*

---

[125] Corte Cost, sentenza n. 372/2006, *considerato in diritto*, §§ 5.1 e 5.2, in cui ci si rifà alle sentt. nn. 81/1993 e 63/1994 (sul bilanciamento tra riservatezza e interesse della collettività alla repressione dei reati).

[126] Corte Cost, sentenza, n. 271/2005, *considerato in diritto*, § 2.

e della riservatezza, ossia quell'insieme di pronunce con cui la Corte costituzionale ha via via tratteggiato i contorni del c.d. «diritto all'identità personale».

Anche questa figura rientra tra quei nuovi diritti della personalità volti garantire adeguate tutele all'individuo rispetto al libero sviluppo della sua personalità nel contesto sociale che lo circonda.

Inizialmente, nelle riflessioni maturate in ambito civilistico, questo diritto è stato letto come l'interesse dell'individuo a veder garantito il patrimonio spirituale, intellettuale e professionale che normalmente lo identifica, soprattutto contro quegli eventi che potrebbero concorre ad alterarlo o falsificarlo contro la sua volontà[127].

Gli studi che in seguito hanno approfondito le implicazioni costituzionali di queste prime intuizioni dimostrano come, anche in questo caso – così come era accaduto per il diritto alla riservatezza – ci si trovi di fronte ad uno scenario estremamente complesso e mutevole [128]. Il soggetto, infatti, rispetto alla rappresentazione di sé stesso, può aver molteplici interessi, anche tra loro contrapposti. Potrebbe desiderare, ad esempio, di essere identificato, così come a rimanere nell'anonimato; di ottenere una rappresentazione completa e veritiera di sé, così come a voler creare identità alternative, a seconda dei diversi contesti. Non da ultimo, tutte queste aspettative possono spiegarsi in molteplici direzioni, toccando ora i diritti tradizionalmente collegati alla tutela del nome e dell'immagine, ora le

---

[127] Anche in questo caso, si tratta di un percorso giurisprudenziale inaugurato dalla Cassazione a partire dagli anni Sessanta. La Suprema Corte, infatti, seguendo le istanze di garanzia espresse ai giudici ordinari, progressivamente comincia a riconoscere tutela all'«esigenza che i fatti, i pensieri, le frasi e le opinioni altri [siano] corrispondenti a verità» (C. Cass., sent. 7 dicembre 1960). A quel primo riconoscimento poi sono seguite ulteriori conferme e specificazioni, estendo i margini di protezione anche a nuove fattispecie. Si rinvia, *ex multis*, a: C. Cass., sent. 22 giugno 1985, n. 3769 (*Veronesi*); C. Cass., sent. 7 febbraio 1996, n. 978. Per un approfondimento su questi sviluppi in ambito civilistico si rinvia, *ex multis*, a G. ALPA, M. BESSONE, L. BONESCHI (a cura di), *Il diritto all'identità personale*, Padova, Cedam, 1981.

[128] Si rinvia, *ex multis*, a G. PINO, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, Il Mulino, 2003; L. TRUCCO, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale*, Torino, Giappichelli, 2004.

aspettative relative ad altre dimensioni del sé, personali o relazionali, statiche o dinamiche[129].

Proprio alla luce di queste considerazioni, la giurisprudenza e la dottrina negli anni stanno continuando ad individuare ulteriori declinazioni del concetto di identità, elaborando – quando meno *de iure condendo* – nuovi e specifici diritti legati alla tutela di questo tipo di prerogative. Il catalogo delle situazioni meritevoli di tutela ne risulta quindi notevolmente ampliato, includendo sempre nuove figure: dal diritto all'identità genetica[130] al diritto all'identità sessuale[131], dal diritto di sapere le proprie origini familiari[132] al diritto di conoscere il proprio destino quando ci si sottoponga a certi trattamenti sanitari[133].

---

[129] Questa la meticolosa ricostruzione del concetto di identità e identificabilità proposto in L. TRUCCO, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale*, cit. *passim*.

[130] Questo diritto, nel tempo, ha trovato alcuni riferimenti impliciti a livello sovranazionale, soprattutto nella Convenzione di Oviedo sui diritti umani e la biomedicina (art. 1) e nella Dichiarazione universale sul genoma umano e diritti umani (artt. 1 e 2), proclamate rispettivamente dal Consiglio d'Europa e dalle Nazioni Unite nel 1997. Parallelamente, sono maturate altre diverse riflessioni sul punto anche a livello nazionale, soprattutto nell'ambito della disciplina sulle tecniche di procreazione medicalmente assistita e sulla ricerca medica sugli embrioni.

[131] In diritto all'identità sessuale, in particolare, è stato oggetto a più riprese dell'attenzione della Corte costituzionale, in particolare con riferimento a quanto deciso nelle recenti sentenze nn. 221/2015 e 180/2017 e nell'ord. n. 185/2017. Per alcune riflessioni sul punto si rinvia, *ex multis*, a C.M. REALE, *Corte costituzionale e trasgendersimo: l'irriducibile varietà delle singole situazioni*, in *Rivista di Biodiritto*, 1, 2016, pp. 289 ss.; C.P. GUARINI, *«Maschio e femmina li creò…» o, forse, no. La Corte costituzionale ancora sulla non necessità di intervento chirurgico per la rettificazione anagrafica di attribuzione di sesso*, in *Federalismi*, 8/2018.

[132] Rispetto al diritto di sapere delle proprie origini familiari, la Corte costituzionale e la Cassazione, anche su impulso della Corte EDU (*Godelli c. Italia* – sent. 25 settembre 2012 (n. 33783/09)) sono tornate più volte, da ultimo, rispettivamente, con la pronuncia n. 287/2013 (Corte cost.) e, *ex multis*, le sentt. del 9 novembre 2016, n. 22838 e 20 marzo 2018, n. 6963. In dottrina, alcune osservazioni, anche rispetto agli orientamenti europei su parto anonimo e procreazione medicalmente assistita eterologa, in: E. VIGATO, *Godelli c. Italia. Il diritto a conoscere le proprie origini*, in *Quaderni costituzionali*, 4, 2012; M. CASINI, C. CASINI, *Il dibattito sulla PMA eterologa all'indomani della sentenza costituzionale n. 162 del 2014. In particolare: il diritto a conoscere le proprie origini e l'"adozione per la nascita"* in *Rivista di Biodiritto,* 2, 2014, pp. 21 ss.; L. BOZZI, *Il diritto di conoscere le proprie origini*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, pp. 1323.

[133] Il c.d. «diritto a conoscere il proprio destino» deve la sua elaborazione soprattutto allo sviluppo dei test genetici predittivi, mediante i quali attraverso l'analisi di specifici campioni genetici è possibile individuare conformazioni o anomalie tali da poter determinare l'insorgere di particolari sindromi o patologie. Una prima disciplina di questi strumenti si ravvede nelle indicazioni che si

Evidentemente una lettura così trasversale dei vari interessi che possono essere ricondotti al concetto di identità individuale è destinata ad intercettare diverse discipline, inclusa certo quella relativa alla protezione dei dati personali. Oltre i tradizionali riferimenti civilistici relativi al diritto al nome e all'immagine personale, alla proprietà intellettuale e al diritto di autore, così come la disciplina sui nomi commerciali e i marchi, con il tempo, la Corte costituzionale, infatti, ha dato maggior solidità ad interpretazioni più incentrate sui profili personalistici, ancorando queste posizioni alla tutela del libero sviluppo della personalità e della dignità umana secondo quanto suggerito dagli artt. 2 e 3 Cost[134]. Pensando ai dati personali, dunque, vale la pena soffermarsi su alcuni punti emersi con particolare chiarezza in alcune pronunce, analizzando soprattutto gli argomenti proposti dal Giudice delle leggi per estendere le tutele tradizionali ai profili di più stretta rilevanza informativa.

Sebbene in queste occasioni non vi sia stata la giusta occasione per affrontare puntualmente le questioni relative all'utilizzo dei dati, la Corte ha avuto modo di constatare come alla tutela dell'identità coincida un equivalente «diritto ad essere sé stessi», da intendersi come il «rispetto dell'immagine di partecipe alla vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l'individuo»[135].

Come posizione di principio, questa prima conclusione, rideclinando il linguaggio dei diritti, consolida all'interno del nostro ordinamento costituzionale

---

rinvengono nella Convenzione di Oviedo (art. 12) e nella Dichiarazione universale sul genoma umano (art. 5). Alcune interessanti considerazioni si possono rinvenire però anche nelle pronunce in cui la Corte costituzionale si è interessata della c.d. diagnosi genetica preimpianto, nell'ambito delle previsioni contenuti nella l. n. 40/2004 (sentt. 96/2015). In dottrina, rispetto a quest'ultimo punto, si rinvia a M.P. IADICICCO, *La diagnosi genetica preimpianto nella giurisprudenza italiana ed europea. L'insufficienza del dialogo tra le Corti*, in *Quaderni costituzionali*, 2/2015; A. D'ALOIA, *L'(ex) 40*, in *Quaderni costituzionali*, 4, 2015.

[134] F. MODUGNO, *I "nuovi" diritto nella giurisprudenza costituzionale*, cit., pp. 9, 13-14, 26-27; G. PINO, *Il diritto all'identità personale*, cit., pp. 162 ss.; L. TRUCCO, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale*, cit., 232 ss.

[135] Un'ulteriore declinazione del diritto all'identità personale che la Consulta ha inteso come (Corte Cost, sentenza n. 13/1994, successivamente ripresa in Corte Cost, sentenza n. 120/2001).

un'importante premessa alla realizzazione di una società democratica e pluralista. Non è un caso che, qui come in altri ambiti, l'attenzione cada proprio su contenuti e proiezioni della personalità particolarmente sensibili, quasi a tracciare un implicito parallelismo con quanto si ritrova nell'art. 3 Cost., circa i possibili motivi di discriminazione e stigma sociale[136]. E proprio su questi presupposti, è interessante esaminare come la Corte abbia affrontato i conflitti emersi in seno alla giurisprudenza costituzionale circa il diritto di rettifica e modifica dei propri dati personali e l'accesso a quelli altrui. Sebbene non si tratti di questioni che intercettato direttamente la disciplina *ad hoc,* queste pronunce offrono infatti validi spunti di riflessione rispetto al bilanciamento degli interessi coinvolti in siffatte vicende.

Come i giudici costituzionali hanno avuto modo di chiarire anche di recente, la sensibilità sociale rispetto al diritto al nome e all'identità di genere tende ad evolvere, riconoscendo nuove istanze volte ad assicurare a ciascuno la libera realizzazione della propria personalità sociale, riaffermando i principi di dignità ed eguaglianza sanciti dalla Carta. In tal senso, dunque, il desiderio di poter ricostruire la propria genesi e così l'identità della madre naturale, dei donatori dei gameti, così come dei fratelli, delle sorelle e degli ascendenti biologici, ha posto non pochi interrogativi circa i contrapposti interessi legati alla conoscibilità di questi dati.

La Corte, affrontando tali questioni ha così cominciato a sviluppare alcune prime considerazioni sul rapporto tra personalità e informazioni, delineando in prospettiva i punti in cui il diritto alla protezione dei dati si lega con la realizzazione di molteplici valori costituzionali.

---

[136] Come già osservato analizzando nel paragrafo 1.3 quanto previsto dall'art. 35 della Costituzione portoghese, le informazioni c.d. calde o sensibili, sono normalmente quelle riconducibili agli aspetti più delicati dell'identità personale; secondo un parallelismo analogo a quello inizialmente tracciato anche nello Statuto dei lavoratori (l. n. 300/1970) nei contenti dell'art. 8.

Il precipitato delle pronunce qui richiamate, chiaramente, va ben oltre le questioni legate alla sola *data protection*[137]. Tuttavia, per gli argomenti proposti, esse contribuiscono a corroborare la tesi per cui siffatta disciplina non può essere ricondotta soltanto ai valori della riservatezza ma – come già osservato – ambisce una più ampia lettura, volta a promuovere la realizzazione dell'individuo nelle diverse dimensioni sociali in cui si colloca intercettando una molteplicità di diritti e interessi.

## 4. La disciplina sulla protezione dei dati personali dalla legge n. 675/1996 al regolamento 679/2016 UE

Gli argomenti proposti dalla giurisprudenza costituzionale, nel tempo, sono stati recepiti e sviluppati dalla normativa di settore. Come accennato, si tratta di una disciplina intervenuta in ritardo rispetto a quanto accaduto in altri ordinamenti. La legge del 1996, infatti, fu adottato nell'urgenza di uniformarsi a quanto previsto dagli accordi di Schengen, così come alle successive riforme della regolamentazione europea.

Passando quindi all'esame della disciplina positiva, non si può fare a meno di notare come nel contesto italiano, la regolamentazione di questa materia sia costituita da diverse stratificazioni normative. Alle fonti nazionali, infatti, si sovrappongo convenzioni internazionali, atti di diritto comunitario e una vasta gamma di documenti e codici che, settore per settore, specificano al dettaglio i

[137] Anche in occasione della sent. 287/2013, infatti, decidendo le questioni relative alla disciplina sul c.d. parto anonimo e al diritto dell'adottato di conoscere le proprie origini, la Corte costituzionale, pur affrontando incidentalmente quanto previsto dall'allora art. 93, comma 7, d.lgs. 196/2003, ha impostato la propria decisione non tanto sulle questioni inerenti la protezione dei dati personali (e così la possibilità di conoscere i dati relativi alla propria nascita solo decorsi 100 anni dal momento del parto), ma sul bilanciamento di interessi tra la posizione della madre e quella del figlio.

principi della disciplina, assecondando così le puntuali esigenze di ogni attività che implichi l'utilizzo dei dati personali.

Ad una prima ricognizione, si osserva come all'interno nel nostro ordinamento l'architettura normativa tracciata dalla prima legge nel 1996 abbia convissuto con le normative di settore così come con gli ampiamenti accorpati nel Codice Privacy (d.lgs. n. 196/2003)[138], fino ad arrivare alle ultime modifiche introdotte dal d.lgs. 108/2018 per l'attuazione del nuovo regolamento europeo sulla protezione dei dati personali del 2016.

Tracciate queste coordinate, in questo paragrafo si andranno ad approfondire i passaggi che hanno segnato l'evoluzione di questa disciplina e dei suoi contenuti, delineando soprattutto i punti di contatto con l'ordinamento europeo. Proprio in ragion di ciò, al termine di questa disanima, verranno proposte alcune annotazioni circa alcuni aspetti critici di questo processo di assimilazione, avendo a mente soprattutto le implicazioni che derivano dalla protezione dei dati sui diritto fondamentali tradizionalmente garantiti dal nostro sistema costituzionale.

### *4.1. La legge n. 675/1996*

Come già anticipato, in Italia la protezione dei dati personali trova una sua prima codificazione nella legge n. 675/1996, specificamente dedicata alla "tutela delle persone e degli altri soggetti rispetto al trattamento dei dati personali".

Un'istantanea di quel momento storico racconterebbe come, prima di allora, fossero già stati proposti vari disegni di legge in materia[139] e di come, tuttavia, per

---

[138] D.lgs. 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali.*

[139] Inizialmente, infatti, dopo le prime normative di settore, tra gli inizi degli anni ottanta e l'inizio degli anni novanta erano stati promossi dei primi disegni di legge più sistematici. Vanno citati, in particolare, le proposte sostenute dagli onn. Accame e Picano (rispettivamente, del 1981 e del 1982), i progetti c.d. Stegagnini e Mirabelli (1982), i d.d.l. proposto dal Min. Martinazzoli nel 1984, lo schema c.d. *Mirabelli-bis* del 1989, per arrivare così alle proposte del 1992 già finalizzate alla

diversi motivi, tutti alla fine si fossero risolti in un nulla di fatto. Lo scarso interesse della classe politica, le forti pressioni esercitate dai gruppi di interesse e, più in generale, l'ostilità dimostrata dagli operatori economici e giuridici per questo tipo di regolamentazione, infatti, avevano sempre concorso a rallentare l'*iter* legislativo[140], tant'è che erano stati disciplinati soltanto quei settori maggiormente esposti all'attenzione pubblica[141].

A forzare questa situazione di stallo è stato soprattutto l'influsso del diritto comunitario. Si è già ricordato come molti Stati europei ormai da anni si fossero dotati di normative organiche su questi temi e di come anche i giudici costituzionali italiani avessero riconosciuto in siffatti principi una conquista di civiltà ormai indispensabile[142].

Nel 1985, dunque, l'adesione all'accordo di Schengen aveva creato i presupposti per accelerare le riflessioni e i lavori che ormai si protraevano da anni.

---

ratifica della Convenzione n. 108 in vista dell'attuazione dell'accordo Schengen. Cfr, *ex multis*, G. BUTTARELLI, *Banche dati e tutela della riservatezza. La* privacy *nella Società dell'informazione*, Milano, Giuffrè, 1997, pp. [106-121]. S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, Cedam, 2006, pp. 107 ss.

[140] Sui motivi e le resistenze all'approvazione della legge si veda R. PAGANO, *Aspetti economici e giuridici delle banche dati*, in *Informativa e diritto*, 1986, pp. 50 ss.

[141] Come osservato, in precedenza gli interventi del legislatore si erano concentrati sui temi più esposti all'attenzione della pubblica opinione, soprattutto in ambito penale e sul trattamento dei dati personali per finalità di pubblica sicurezza e di salute pubblica e igiene (Cfr. G. BUTTARELLI, *Banche dati e tutela della riservatezza*, cit., pp. [106-109]) In una rapida ricognizione, sono da ricordare soprattutto gli artt. 4 e 8 dello Statuto dei lavoratori (l. n. 300/1970), le prime norme ad aver vietato l'utilizzo di sistemi audiovisivi e di altre apparecchiature di controllo sull'attività dei lavoratori e lo svolgimento di indagini sulle opinioni politiche, religiose e sindacali del lavoratore; le novelle al codice penale di cui agli artt. 615*bis* ss. in materia di interferenze illecite nella vita privata (l. n. 98/1974), accesso abusivo ai sistemi informatici, detenzione e diffusione abusiva di codici di accesso e diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (l. n. 547/1993); la disciplina sulle intercettazioni nell'ambito del nuovo codice di procedura penale del 1989 (spec. artt. 270-271 c.p.p.); la legge n. 121/1981 in tema di raccolta e di elaborazione di dati per finalità di pubblica sicurezza e, in ambito medico-sanitario, le leggi nn. 135 e 309 del 1990 che introducono il diritto a che non vengano divulgati i dati relativi alle infezioni da HIV e alla tossicodipendenza (Cfr. G.M. SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in R. NANIA, P. RIDOLA (a cura di), *I diritti costituzionali*, Torino, Giappichelli, 2006, pp. 621-622).

[142] Corte Cost, sent. 139/1990, *considerato in diritto*, § 11.

Nella prospettiva di abolire le frontiere e di creare un'unione doganale, si sarebbe infatti resa necessaria un'ancor più intesa condivisione di dati e informazioni. E il Trattato, in tal senso, aveva già previsto la creazione di un sistema automatizzato per la gestione dei dati e, con questo, l'istituzione di un'Autorità garante di controllo comune (tutta una serie di meccanismi che, di lì a pochi anni, si sarebbe ulteriormente estesa, soprattutto con il progressivo ampliarsi delle competenze europee).

Alla luce di queste considerazioni, un'adeguata disciplina sulla protezione dei dati personali risultava essere una condizione necessaria per poter effettivamente partecipare all'attuazione dell'accordo. Come si è rilevato, infatti, lo scambio necessitato di informazioni, non solo in ambito economico-privato ma anche e soprattutto per l'adempimento di funzioni pubbliche, rendeva imprescindibile l'adozione di un *framework* normativo condiviso, in modo tale da poter assicurare ovunque un livello minimo di garanzie.

A distanza di dieci anni, dunque, anche sulla spinta della neo-approvata direttiva 46/95 CE, in Italia si è arrivati finalmente all'approvazione della legge del 1996 sulla protezione dei dati, portando così a compimento quella lunga gestazione che ormai si protraeva attraverso le diverse legislature.

L'analisi dei contenuti dell'atto impone una preliminare considerazione. In questa materia il legislatore nazionale (ora come allora) disponeva di un margine di discrezionalità relativamente ridotto. La direttiva in questione, infatti, aveva introdotto una disciplina molto dettagliata, volta a definire secondo i principi europei una considerevole quantità di aspetti. In tal senso, dunque, ad una rapida ricognizione, non si può fare a meno di notare come l'ordinamento nazionale abbia assimilato in una sola volta una vasta gamma di tutele.

Prima di soffermarsi sui profili di maggior interesse, vale la pena di fotografare la struttura di questo complesso normativo. Emulando molti aspetti dell'architettura della direttiva, la legge si compone di 45 articoli, suddivisi in dieci capi. Dopo i

principi generali, si passa alla definizione degli obblighi per il titolare e delle regole per il trattamento dei dati, individuando i diritti dell'interessato, le misure di sicurezza e le condizioni per la comunicazione e la diffusione dei contenuti a terzi. Alla disciplina generale si aggiungono poi alcune previsioni relative al regime di tutela dei dati sensibili, stabilendo condizioni specifiche per alcuni particolari attività di trattamento. Per rendere effettivo quanto previsto dall'impianto normativo così descritto, il testo si concludeva con le norme relative alla tutela amministrativa e giurisdizionale, i poteri dell'autorità garante e il regime sanzionatorio.

Ad un esame più dettagliato, si coglie come la legge del 1996 si ponesse come principale obiettivo quello di garantire che il trattamento dei dati personali si svolgesse nel rispetto dei diritti, della dignità e delle libertà fondamentali dell'individuo, mettendo in chiaro soprattutto la tutela della riservatezza e dell'identità personale[143]. La dottrina, dal punto di vista concettuale, subito soffermandosi su questi aspetti, ha quindi intravisto in questa dichiarazione d'intenti un primo riconoscimento legislativo di una qualche forma di "libertà informatica"; un concetto che già da alcuni anni era stato inteso come una *summa* delle diverse aspettative di tutela contro i rischi di nuove forme di sorveglianza elettronica[144].

Nonostante questi primi accenni al rapporto tra diritti e dati, continuando l'esame della disciplina, non si può fare a meno di notare come questa si componga di un insieme di strumenti che richiamano molto più da vicino quella nozione

---

[143] Art. 1, comma 1, che circa i fini dispone puntualmente: «la presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all´identità personale; garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o associazione».

[144] Una teoria la cui paternità viene normalmente ricondotta all'opera di Vittorio Frosini, per cui si rimanda, *ex multis*, a ID., *La protezione della riservatezza nella società informatica*, in *Informatica e diritto*, 1981; ID. *1984. L'informatica nella società contemporanea* (I e II), *ibidem*, 1981 e 2001; ID., *Banche dati e tutela della persona*, in *Informatica diritto e società*, 1988. Un concetto poi ripreso anche in T.E. FROSINI, *Liberté, Egalité, Internet*, Napoli, Editoriale Scientifica, 2015, *passim*.

allargata di *privacy* cui tanta letteratura aveva già dato seguito[145], intendendo la protezione dei dati soprattutto come un insieme di obblighi e diritti volti a garantire la sicurezza dei contenuti trattati e il controllo sul loro utilizzo. Il legislatore italiano, in particolare, impronta l'attività di trattamento a principi europei ormai consolidati da anni, imponendo al titolare, accanto agli oneri di trasparenza e correttezza, il dovere di assicurare la qualità dei dati utilizzati e a limitarne l'uso alle sole finalità dichiarate, notificando all'interessato la natura delle sue attività e i relativi diritti.

Particolare attenzione, poi, è dedicata alla posizione del soggetto interessato. L'intera disciplina, infatti, insiste sulla necessarietà del consenso (requisito escluso soltanto in alcuni settori particolari con la promessa di assicura *ex lege* adeguate garanzie) riconoscendo quindi una serie di diritti specifici circa i poteri di intervento rispetto ai diversi utilizzi delle informazioni che lo riguardano. In particolare, vengono sanciti definitivamente come diritti l'interesse a conoscere l'esistenza delle banche dati, le prerogative di accesso al registro dei trattamenti e ai dati personali, il potere di rettifica, cancellazione e anonimizzazione, così come il diritto a bloccare i trattamenti illeciti.

Infine, anche in questo settore viene prevista l'istituzione di un'Autorità garante; un ente preposto essenzialmente a promuovere e vigilare sulla corretta attuazione della disciplina e sull'effettiva tutela dei diritti legati all'utilizzo dei dati.

Guardando all'ambito di applicazione di questa prima legge, non si può fare a meno di notare come, proprio per la sua portata generale, essa fosse destinata a trovare spazio tanto nell'attività dei soggetti pubblici quanto di quelli privati, intercettando così una vastissima area di fenomeni. La disciplina del 1996 segna quindi un punto di svolta nell'evoluzione della normativa sulla protezione dei dati

---

[145] In particolare, S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, cit.; ID., *La privacy tra individuo e collettività,* in *Politica del diritto,* 1974, 5, pp. 545 ss.; ID., privacy *e costruzione della sfera privata. Ipotesi e prospettive*, in *Politica del diritto*, 1991, pp. 521 ss. Con lui, comunque, in quegli stessi anni, merita menzione anche il pensiero di C. MIRABELLI, *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, cit., p. 313 ss.

personali. Essa non solo introduce per la prima volta una disciplina sistematica dell'intera materia ma adegua i meccanismi di tutela degli interessi legati a queste attività ad una serie di principi e standard di matrice europea in un'epoca in cui le competenze comunitarie in materia di diritti fondamentali erano ancora controverse.

### *4.2. Il D.lgs. n. 196/2003 o Codice Privacy*

La situazione descritta nelle pagine precedenti con riferimento alla legge n. 675/1996, ha trovato piene e ulteriori conferme negli anni successivi, quando il *corpus* originario di questa disciplina, ha registrato una notevole espansione – qualitativa e quantitativa – soprattutto su impulso del legislatore europeo.

Con l'intento di incentivare in modo sempre più deciso lo sviluppo del mercato unico digitale, oltre alla direttiva n. 46/95, la Commissione infatti è intervenuta a più riprese con dei nuovi interventi normativi, volti soprattutto a promuovere una maggior armonizzazione della disciplina nazionale nei diversi settori coinvolti dalla digitalizzazione.

Dopo la proclamazione della Carta di Nizza, in particolare, a completamento del quadro normativo comunitario[146] erano state aggiunte le direttive nn. 58/2002 e 24/2006 CE: l'una relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche; l'altra riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di

[146] Questi i principali apporti all'evoluzione della disciplina europea, come rappresentato anche in F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali,* vol. I, *Dalla direttiva 96/46 al nuovo Regolamento europeo*, Torino, Giappichelli, 2016, pp. 128 ss. In precedenza, tuttavia, era stata introdotta anche la direttiva n. 66/97 CE sulle comunicazioni elettroniche, con cui erano stati disciplinati anche alcuni importanti aspetti sulla protezione dei dati personali legati all'utilizzo dei sistemi, ai contenuti delle comunicazioni e alle condizioni per il trattamento delle informazioni necessari alla fatturazione. I riferimenti sono: Direttiva 97/66/CE del Parlamento europeo e del Consiglio del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni; per un primo commento in dottrina v. P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione europea*, Milano, Giuffré, 2002, pp. 177 ss.

comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, recante alcune modifiche alla disciplina della prima[147].

Alla luce di queste novità e dei ripetuti interventi del legislatore nazionale a completamento della l. n. 675/1996, la disciplina di quest'ultima e le successive *addenda*[148] hanno così trovato una loro definitiva collocazione nel c.d. Codice privacy, introdotto con il d.lgs. n. 196/2003[149].

Confrontando i due testi, si colgono immediatamente evidenti differenze. La struttura del nuovo articolato risulta profondamente ampliata e rivista, includendo e disciplinando *ex lege* nuove categorie di trattamento. L'architettura normativa ora si regge su tre parti, rispettivamente dedicate alle disposizioni generali, alla disciplina relativa ad alcuni settori specifici e alla tutela dell'interessato, per un totale di ben oltre 180 disposizioni.

A parte l'evidente differenza nella quantità di articoli, si colgono subito e in modo ancor più evidente gli influssi del diritto europeo e, in particolare, del neo-

---

147 Sui contenuti e sull'apporto di questi atti normativi allo sviluppo della strategia di *data governance* europea si tornerà con maggior dettaglio nel capitolo 3.

148 Tra i principali interventi – come sottolineato in E. GROSSO, *Autorità indipendente o autorità onnipotente? Il potere normativo di fatto del garante per la protezione dei dati personali,* in M. LOSANO (a cura di), *La legge italiana sulla* privacy, cit., p. 139, nota 1 – vanno ricordate le modifiche apportate dai seguenti atti normativi: d.lgs. 9 maggio 1997, n. 123, recante *Disposizioni correttive ed integrative della legge 31 dicembre 1996) n. 675) in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*; d.lgs. 28 luglio 1997, n. 255, recante *Disposizioni integrative e correttive della legge 31 dicembre 1996) n. 675, in materia di notificazione dei trattamenti di dati personali a norma dell'articolo 1, comma 1) lettera f), della legge 31 dicembre 1996, n. 676*; d.lgs. 8 maggio 1998, n. 135, recante *Disposizioni in materia di trattamento di dati particolari da parte di soggetti pubblici*; d.lgs. 13 maggio 1998, n. 171, recante *Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attività giornalistica*; d.lgs. 6 novembre 1998, n. 389, recante *Disposizioni in materia di trattamento di dati particolari da parte di soggetti pubblici*; d.lgs. 26 febbraio 1999, n. 51, recante *Disposizioni integrative e correttive della legge 31 dicembre 1996, n. 675) concernenti il personale dell'ufficio del Garante per la protezione dei dati personali*; d.lgs. 11 maggio 1999, n. 135, recante *Disposizioni integrative della legge 31 dicembre 1996, n. 675, sul trattamento di dati sensibili da parte dei soggetti pubblici*; d.lgs. 30 luglio 1999, n. 281, recante *Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica*; d.lgs. 30 luglio 1999, n. 282, recante *Disposizioni per garantire la riservatezza dei dati personali in ambito sanitario*.

149 A commento, *ex multis,* S. SICA, P. STANZIONE (a cura di), *La nuova disciplina della privacy. Commento al d.lgs. 30 giugno 2003, n. 196*, Bologna, Zanichelli, 2005; V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Torino, Giappichelli, 2007.

introdotto art. 8 CDFUE. L'art. 1 del nuovo "testo unico", apre affermando infatti che «chiunque ha il diritto alla protezione dei propri dati», così sancendo anche a livello nazionale quell'autonomia concettuale tra *privacy* e *data protection* sancita qualche anno prima dalla Convenzione di Nizza.

Per quanto riguarda la parte generale, i contenuti essenziali, tutto sommato, hanno mantenuto una certa stabilità, magari specificando meglio alcuni profili di dettaglio e ribadendo il valore centrale dei principi e dei diritti consacrati dalla direttiva del 1995.

Più innovative, invece, sono le parti in cui il legislatore ha provveduto a definire le norme necessarie allo svolgimento delle attività di trattamento in alcuni settori particolari. L'elenco è lungo, la legge molto articolata. Ai trattamenti in ambito giudiziario, da parte delle forze di polizia – e, più in generale, per la difesa e la sicurezza dello Stato – si passa alla disciplina relativa al settore pubblico: dall'accesso agli atti, ai registri pubblici, all'anagrafe e lo stato civile, alle molte altre attività necessarie per finalità di pubblico interesse. Segue una dettagliata regolamentazione in materia di dati sanitari (dati sensibili per eccellenza), unitamente alle prescrizioni relative al settore dell'istruzione e della ricerca storica, scientifica e statistica. Infine, vi sono le regole relative al trattamento dati nell'ambito dei rapporti di lavoro e ai fini delle prestazioni di previdenza sociale, per il sistema bancario e per il ramo delle assicurazioni e per le comunicazioni elettroniche.

In questa breve panoramica, quel che colpisce è che, a differenza del passato, pur continuando a promuovere forme di regolamentazione concertata in diversi settori (soprattutto attraverso i codici di deontologia e buona condotta) l'obiettivo del decreto sia quello di dare all'intera materia un'impostazione quanto più possibile unitaria e sistematica. Il legislatore, cioè, oltre ad individuare dei principi di portata generale, secondo i canoni di un metodo casistico, individua *ex lege,* le regole di una disciplina più specifica, riconducendo regole ed eccezioni an un quadro normativo unitario, in cui possono essere ricomposti gli eventuali dissidi tra interessi

contrapposti.

Come osservato da alcuni, che per ciascun ambito venga delimitata e circoscritta la «topografia del conflitto»[150], secondo una logica non dissimile da quella utilizzata nei giudizi di costituzionalità. Il legislatore, sulla base di una serie di principi di portata generale, seleziona gli interessi che, in prospettiva, devono trovare un giusto bilanciamento, individuando così i criteri di un «bilanciamento-regola». Alla luce di questo primo risultato, poi, attraverso una serie di eccezioni, determina anche una serie di elementi che *in negativo*, definiscono dei criteri di «bilanciamento-deroga»[151].

In altri termini, tutte le operazioni di bilanciamento che, fino a quel momento, avevano chiesto un'attenta opera di ponderazione da parte degli interpreti, ora trovano puntuali riferimenti all'interno del Codice, come a ribadire la centralità di questa materia e dei suoi principi rispetto alla disciplina tradizionale di settore e la forza centripeta dei paradigmi assimilati dal diritto europeo su quelli propri dell'esperienza nazionale.

Ciò considerato, l'impianto generale della disciplina, come assestatosi nel 2003, è quello che, pur con frequenti modifiche, è giunto fino ai tempi più recenti. E le scelte operate all'epoca, nel tempo, sembrano aver trovato il plauso della Corte costituzionale. Pur essendoci stata occasione per saggiare la legittimità di alcune norme del Codice, non è emersa una giurisprudenza particolarmente incisiva: i giudici costituzionali, pur accogliendo i principi e diritti sanciti da questa normativa,

---

[150] . MASSO PINTO, *Il bilanciamento degli interessi nella legge sulla privacy*, cit., pp. [95-99] spec. nota 7. Si osserva infatti: «poiché la formula «topografia del conflitto» è stata coniata con riferimento all'attività preliminare compiuta dalla Corte costituzionale, sembra sottintendersi che anche la preventiva selezione degli interessi da ammettere al bilanciamento sia frutto di una scelta discrezionale del giudice delle leggi. In realtà l'individuazione degli elementi da bilanciare è il risultato di un complesso ragionamento che impegna la Corte nella ricerca della *ratio* della norma impugnata, ma è quest'ultima che seleziona implicitamente gli interessi che intende tutelare (ovvero che intende sacrificare per tutelarne altri). Secondo questa ricostruzione teorica la Corte dovrebbe limitarsi a identificare gli interessi in concorso che hanno ispirato la norma impugnata». Più diffusamente, sulla «topografia del conflitto», in generale, si rimanda anche a R. BIN, *Diritti e argomenti: il bilanciamento degli interessi nella giurisprudenza costituzionale*, Milano, Giuffrè, 1992, pp. 62 ss.

[151] *Ibidem*, p. 95.

non hanno mancato di sottolineare come si tratti di una «discendenza comunitaria» e, per le questioni che le sono state rivolte, di norma si è limitata a confermare la discrezionalità del legislatore rispetto alle modalità e i criteri della sua attuazione.

### *4.3. I primi adeguamenti al reg. 679/2016 con il d.lgs. 101/2018*

Il quadro normativo descritto nel paragrafo precedente, in tempi recenti, ha però subito un drastico cambiamento, soprattutto in seguito all'adozione del nuovo regolamento generale europeo per la protezione dei dati personali (reg. 679/2016) [152].

---

[152] Sulle iniziative di consultazione precedenti alla proposta di regolamento, si ricordano, *ex multis,* la conferenza *Personal data: more use, more protection*, organizzata a Bruxelles dalla Commissione nel maggio 2009; il parere redatto dal Gruppo Articolo 29, *The Future of Privacy: Joint contribution to the Consultation in the European Commission on the legal framework for the fundamental right to protection of personal data* (WP n. 168) del 1° dicembre 2009; la Comunicazione della Commissione al Parlamento europeo, al Consiglio, la Comitato economico e sociale europeo e al Comitato delle regioni, *Un approccio globale alla protezione dei dati personali nell'Unione Europea*, Bruxelles, 4 novembre 2010. Per una più ampia panoramica su questi sviluppi, v. F. PIZZETTI, *Sette anni di protezione dei dati in Italia,* Torino, Giappichelli, 2012, Parte IV, *L'evoluzione della normativa europea in tema di protezione dei dati personali.*

Per una rapida panoramica, soprattutto rispetto ai punti di intersezione tra la precedente disciplina e il nuovo reg. 679/2016, si rimanda a F. PIZZETTI, *Privacy e il diritto europea alla protezione dei dati personali*, vol. II, *Il Regolamento europeo 2016/679*, Torino, Giappichelli, pp. 14-15) e rispetto alla strategia di c.d. *data governance* europea oltre al reg. n. 679/2016 si richiamano anche: le dirr. nn. 680/2016 UE («*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 e che abroga la decisione quadro 2008/977/GAI del Consiglio*») e 681/2016 UE («*sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi*»). Sono inoltre oggetto di attuale revisione la dir. CE 58/2002 («*relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche*», già oggetto di modifica ad opera della dir. n. 136/2009 UE e oggi in discussione rispetto al proposal COM(2017) 10) e la dir. CE 58/2004 («*sul rispetto dei diritti di proprietà intellettuale*», questa relativamente solo ad alcuni profili – proposal: COM/2016/0593). A corollario vi sono infine le direttive UE 98/2003 e UE 98/2013 («*relativa al riutilizzo dell'informazione del settore pubblico*», il cui testo definitivo è già stato approvato dal Parlamento europeo). A tutto ciò si aggiunge, peraltro, la già ricordata proposta di regolamento in materia di dati non personali (proposal: COM/2017/0495, i cui sviluppi, tuttavia, sono ancora incerti).

Dal 2012 ad oggi, la Commissione e il Parlamento europeo hanno promosso una profonda riforma della disciplina sulla protezione dei dati personali, inaugurando una nuova strategia di *data-governance* che sta rivoluzionando non solo il diritto dell'Unione ma anche quello degli Stati membri. Negli ultimi anni, infatti, lo sviluppo di molti nuovi servizi digitali e la potente accelerazione registrata in tutto il settore delle ICT e delle tecnologie *data-intensive* è stato motivo di nuove preoccupazioni, in particolare per quanto riguarda il rapporto tra diritti e dati personali.

A documentare l'impatto di questi mutamenti sul piano del diritto sono soprattutto i numerosi pareri richiesti via via al Gruppo di lavoro Articolo 29[153]. La rapida diffusione dei dati sui *social network* online*,* nei servizi *cloud,* e per le infinite applicazioni disponibili per i dispositivi mobili[154], le innovazioni registrate nel campo dei sensori e dei sistemi di tracciabilità, i progressi dell'intelligenza artificiale e dell'internet delle cose[155], infatti, non solo hanno dato piena prova di quello che può essere il potenziale della c.d. *data economy* ma – in parallelo – hanno cominciato a

---

[153] Il Gruppo articolo 29 è un organo con funzioni regolamentari e consultive istituito sulla base di quanto previsto, per l'appunto, dall'art. 29, dir. 46/95 CE ed oggi sostituito nei suoi principali compiti dal Comitato europeo per la protezione dei dati personali (meglio noto come EDPB, *European Data Protection Board*) secondo quanto disposto dall'art. 70, reg. 679/2016. Per un approfondimento, si rinvia, *ex multis*, a V. ZEMBRANO, *Il Comitato europeo per la protezione dei dati*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, pp. 983 ss; F. PIZZETTI, *Privacy e il diritto europea alla protezione dei dati personali*, vol. II, *Il Regolamento europeo 2016/679*, cit., pp. 103 ss.

[154] Gruppo Articolo 29, parere del 4 aprile 2008, *Opinion 1/2008 on data protection issues related to search engines* (WP138); parere del 12 giugno 2009, *Opinion 5/2009 on online social networking* (WP163); parere del 22 giugno 2010, *Opinion 2/2010 on online behavioral advertising* (WP171); parere del 6 maggio 2011, *Opinion 13/2011 on Geolocation services on smart mobile devices* (WP185); parere del 22 marzo 2012, *Opinion 02/2012 on facial recognition in online and mobile services* (WP192); parere del 27 aprile 2012, *Opinion 3/2012 on developments in biometric technologies* (WP193).

[155] ID, parere 1 luglio 2012, *Opinion 05/2012 on Cloud Computing* (WP196); parere del 27 febbraio 2013, *Opinion 02/2013 on apps on smart devices* (WP202); parere 6 giugno 2013, *Opinion 05/2013 on Smart Borders* (WP206); parere del 4 dicembre 2013, *Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force* (WP209); parere 16 settembre 2014, *Opinion 8/2014 on the on Recent Developments on the Internet of Things* (WP223).

sollevare non poche perplessità circa l'adeguatezza dello storico sistema di garanzie istituito nel 1995.

Si è reso così necessaria una profonda revisione della disciplina (che tutt'ora perdura) e il primo risultato concreto di questo progetto di riforma è senz'altro reg. 679/2016 UE, il Regolamento generale sulla protezione dei dati personali (GDPR)[156] con cui si è sostituita la precedente direttiva.

Le ragioni che hanno indotto a ripensare il quadro di tutele sulla *privacy*, passando da sistema basato sulle direttive ad uno incentrato su un regolamento, chiaramente, sono molteplici. Si possono però individuare due punti principali: il bisogno di aggiornare il quadro complessivo della normativa per poter avere regole al passo con lo sviluppo delle tecnologie e l'esigenza di imprimere una spinta più decisa al processo di armonizzazione della disciplina su questi temi a livello europeo[157].

In seguito ci sarà il modo di approfondire meglio i contenuti e le novità introdotte dalla recente riforma. Quello che però va subito riscontrato è che, con questo passaggio da una direttiva ad un regolamento, il baricentro della disciplina sulla protezione dei dati personali, già in precedenza "sbilanciato" verso una lettura filo-comunitaria, si sposta definitivamente verso Bruxelles, trovando nelle regole approvate in sede europea la matrice di riferimento per la tutela dei diritti coinvolti dal trattamento dei dati.

Ed è in quest'ottica che torna in primo piano quanto poc'anzi accennato rispetto alla natura di queste previsioni; alla loro attitudine ad essere criterio di

---

[156] Secondo l'acronimo della versione inglese, *General Data Protection Regulation.*

[157] L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2017, pp. 17 ss. Come osservato anche dalla Commissione, infatti, la direttiva, pur costituendo la «pietra angolare» della privacy (Cfr. COM(2012) 11 final, p. 1) non era stata in grado di evitare del tutto la frammentazione della disciplina, specie a fronte dell'ampiamento stesso dell'Unione, con l'ingresso di nuovi Stati membri dall'Est Europa. Sul punto, v. D. VANNI, *La protezione dei dati personali in prospettiva comparatistica*, Roma, Aracne, 2012.

bilanciamento operativo per procedere al corretto contemperamento degli interessi legati e contrapposti nell'ambito di una medesima attività di trattamento. Questa migrazione verso l'alto del sistema di garanzie e delle fonti del diritto può sollevare più di qualche interrogativo, soprattutto riflettendo sul ruolo che oggi spetta al legislatore nazionale e alla Corte costituzionale rispetto alla tutela dei diritti fondamentali intercettati da questa rivoluzione dell'informazione.

Senza dubbio, nulla vieta che la legge statale possa integrare e chiarire i contenuti della disciplina oggetto di un regolamento[158], e questo vale maggior ragione nei casi in cui sia proprio il legislatore europeo a prevedere una simile eventualità, proprio come sancito dal il reg. 679/2016.

Già scorrendo rapidamente il testo dei *considerando*, si legge come sia il GDPR stesso a prevedere integrazioni e limitazioni ad opera degli Stati membri, e questo in molti ambiti: dalla definizione delle situazioni di legittimità del trattamento, alla definizione di ulteriori garanzie per l'utilizzo dati sensibili, fino alla regolamentazione di alcuni interi settori. È interessante notare come, accanto alle specificazioni e agli adempimenti di tipo tecnico e istituzionale, il legislatore europeo abbia previsto la possibilità di integrare la normativa comunitaria proprio in quegli ambiti in cui il bilanciamento degli interessi in gioco presenta sfumature critiche, come, ad esempio, nel campo delle attività d'informazione, della sicurezza nazionale,

[158] La Corte di Giustizia, infatti, ha riconosciuto già a partire dagli anni Settanta la possibilità di intervenire con disposizioni attuative o integrative alla disciplina predisposta dai regolamenti, purché questo non si traduca in un ostacolo all'attuazione del regolamento medesimo o in un'eccessiva differenziazione del dato normativo. In tal senso, dunque, sono state elaborate due indicazioni di massima: da un lato, il diritto interno può integrare il diritto europeo previsto da un regolamento solo ove quest'ultimo lo preveda e soltanto nei limiti dello strettamente necessario; dall'altro, ove si rendano necessarie norme interpretative, queste possono concorrere all'applicazione della disciplina comunitaria ma non possono avere carattere obbligatorio. (Cfr. CGUE, sent. 11 febbraio 1971, C-39/70, *Norddeutsches Vieh-und Fleischkontor v. Hauptzollamt Hamburg St Annen*; sent. 31 gennaio 1978, C-94/77, *Fratelli Zerbone Snc v. Amministrazione delle finanze dello Stato;* sent. 21 dicembre 2011, C-316/10, *Danske Svineproducenter v. Justitsministeriet*).

della protezione sociale e della ricerca scientifica[159]. Come si osserva, potrebbe trattarsi di adattamenti tanto *in melius* quanto *in peius* rispetto ai livelli di tutela generalmente previsti dalla normativa comunitaria. Le uniche condizioni sono che gli interventi siano finalizzati a rendere più coerente e comprensibile l'applicazione della normativa, che venga comunque rispettato il contenuto essenziale dei diritti fondamentali e che le misure restrittive siano assistite da riserva di legge e risultino necessarie e proporzionate rispetto ai fini che si intendono perseguire.

Il nuovo quadro normativo, dunque, pur invertendo la logica propria delle direttive, prevede comunque un regime di concorrenza tra fonti, mettendo subito in chiaro come il fine ultimo di questa disciplina sia quello di promuovere un equo bilanciamento fra gli interessi costituzionalmente garantiti dal diritto europeo e dal diritto nazionale.

Nel contesto italiano, tuttavia, queste indicazioni sono state accolte e recepite in modo alquanto turbolento. Parte degli adattamenti necessari sono stati introdotti in tutta fretta con il d.lgs. 101/2018[160], un atto che, sebbene gli ampi termini di adeguamento, è sopravvenuto ben oltre le scadenze previste da Bruxelles[161].

---

[159] Sono le indicazioni che si rinvengono soprattutto nel capo IX, relativamente alle *Disposizioni relative a specifiche situazioni di trattamento*, in cui sono previste normative *ad hoc* in materia di libertà d'espressione e di informazione (art. 85), accesso del pubblico ai documenti ufficiali (art. 86), numero di identificazione nazionale (art. 87), nell'ambito dei rapporti di lavoro (art. 87), a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici (art. 88), sugli obblighi di segretezza (art. 89) e, più in generale, sulle norme di protezione dei dati vigenti presso chiese e associazioni religiose (art. 90).

[160] Da un punto di vista tecnico, l'intervento di adeguamento si articola in più atti e disposizioni: la legge 25 ottobre 2017, n. 163 – «*Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2016-2017*» – all'art. 13, prevede una delega al Governo per l'adeguamento della normativa nazionale al regolamento (UE) n. 2016/679, per quanto attiene i contenuti normativi; la legge 20 novembre 2017, n. 167 – «*Disposizioni per l'adeguamento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea – Legge europea 2017*» – stanzia invece le risorse necessarie ad incrementare la dotazione economica e organizzativa necessaria per garantire la piena operatività dell'Autorità garante secondo le nuove funzioni previste dal Regolamento.

[161] Il regolamento, infatti, aveva imposto l'adeguamento della disciplina entro il 25 maggio 2018, lasciando così agli Stati membri più di due anni di tempo per procedere all'adeguamento delle loro discipline interne; contestualmente, lo scadere del termine avrebbe a tutti gli effetti abrogato la

Nonostante la Commissione ministeriale incaricata del progetto inizialmente avesse valutato l'opportunità di un intervento che andasse a sostituire *in toto* la precedente disciplina, alla fine si è optato per una risistemazione del vecchio Codice Privacy, giustificando tale scelta con l'intenzione di conservare e promuovere l'unitarietà del tradizionale impianto normativo[162].

Considerati i tempi in cui il d.lgs. 101/2018 è stato concepito, sembra quasi inutile constatare come la fretta sia stata fatale al risultato. Guardando a quel che resta dell'impianto del vecchio Codice, il testo normativo si è ridotto a soli 27 articoli, suddivisi in sei capi non del tutto omogenei.

La struttura originaria, come osservato in alcune prime recensioni, è andata in larga parte perduta, riorganizzando la disciplina in modo frammentario e discontinuo. Nell'ambito delle disposizioni generali una lunga lista di previsioni specifica il rapporto tra regolamento e diritto interno circa i principi e la finalità della disciplina e il ruolo delle autorità di controllo. Seguono quindi una serie di norme sulle basi giuridiche del trattamento e le regole deontologiche, seguite dalle

---

precedente disciplina (art. 94). Così come era stato in passato, tuttavia, il legislatore italiano si è dimostrato inerte rispetto alle incombenze di sua spettanza, affidando la delega al governo solo sul finire del 2017. A questo e altri ritardi, dunque, si deve il fatto che il primo d.lgs. attuativo – in n. 101/2018 – sia intervenuto ben oltre i termini previsti dall'art. 94, solamente il 10 agosto 2018. Circa l'*iter* di approvazione, v. V. CUFFARO, *Quel che resta di un codice: il D.lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del Codice della Privacy al Regolamento sulla protezione dei dati*, in *Corriere giuridico*, n. 10, 2018, § 2.

[162] Inizialmente queste sembravano le intenzioni, in linea anche – e soprattutto – con gli obiettivi indicati dal *considerando 8* in cui si prevede che «Ove il presente regolamento preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, gli Stati membri possono, nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone cui si applicano, integrare elementi del presente regolamento nel proprio diritto nazionale».

Quanto alla scelta di procedere alla revisione della precedente, si potevano considerare diverse opzioni. Se alcuni Stati, come la Francia, hanno deciso di procedere in modo graduale, implementando la disciplina in diversi provvedimenti, in altri ordinamenti – ad esempio, in Germania e in Austria – le precedenti leggi sono state completamente abrogate e sostituite ben prima dello scadere dei termini indicati dal regolamento; un orientamento, seguito poi anche da altri Paesi, come la Spagna. Cfr. M. RUBECHI, *La transizione verso il nuovo sistema delle fonti europee di protezione dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., pp. [387-392].

condizioni di validità del consenso del minore e il trattamento di particolari categorie di dati (soprattutto quanto avvenga per finalità di interesse pubblico)[163].

A completamento del *bill of rights*[164] previsto dal regolamento, seguono le limitazioni ai diritti dell'interessato e gli obblighi in capo al titolare del trattamento, ma non ulteriori e più puntuali garanzie a favore dei soggetti direttamente o indirettamente coinvolti in queste attività. Segue la parte dedicata alle attività necessarie all'adempimento ai compiti di pubblico interesse o che coinvolgono profili particolarmente delicati, introdotta da un "curioso" *Titolo 0.1* relativo alla base giuridica. Individuate le situazioni che, in generale, rendono legittime alcune particolari attività di trattamento e la relativa disciplina, della normativa di settore però rimangono solo le previsioni relative alla informatica giuridica in ambito giudiziario, alla difesa e alla sicurezza dello Stato, all'accesso ai documenti amministrativi e all'utilizzo dei dati pubblici, recuperando poi, qui e là, qualcosa della disciplina in materia di sanità, istruzione e ricerca, in campo assicurativo e lavoristico e per le attività d'informazione e comunicazione[165].

---

[163] Qui nella prima parte, in una complicata rinumerazione dell'art. 2, si trovano come principi generali le norme sulla base giuridica dei trattamenti effettuati per compiti di pubblico interesse o connessi all'esercizio di pubblici poteri (art. 2*ter*), le regole deontologiche (art. 2*quater*), il consenso del minore (art. 2*quinquies*), alcune norme sul trattamento di particolari categorie di dati (artt. 2*sexies*, 2*septies*, 2*octies*) e la disciplina dei trattamenti regolati dalla Presidenza della Repubblica, dalla Camera dei Deputati, dal Senato della Repubblica e dalla Corte costituzionale (art. 2*novies*). Segue, al titolo 0.1 (*sigh!*) le disposizioni relative alla base giuridica (art. 45*bis*).

Seguono le condizioni di inutilizzabilità dei dati (art. 2*decies*); le limitazioni ai diritti dell'interessato (artt. 2*undecies*, 2*duodecies*, 2*terdecies*); alcune previsioni relative alla posizione del titolare del trattamento, quali le deleghe e le attribuzioni di funzioni ad altri soggetti designati (art. 2*quinquiesdecies*) e i trattamenti per l'esecuzione di un compito di interesse pubblico che presentano gravi margini di rischio (art. 2*sexiesdecies*).

[164] Si allude alle previsioni contenute agli articoli relativi ai diritti di conoscere e consentire al trattamento (artt. 13-15), al diritto di accesso (art. 15), di cancellazione, rettifica e limitazione del trattamento (artt. 16-18), così come ai diritti alla portabilità dei dati e di opposizione al trattamento e alla profilazione (artt. 20-21 e 22, § 1), nonché l'alquanto discusso diritto ad una spiegazione (art. 22, § 2, *considerando* 63).

[165] Una ricostruzione organica delle prescrizioni risulta comunque ostica anche all'interno delle area più omogenee. L'art 27 del d.lgs. infatti prevede una serie di tagli diagonali che incidono sulla disciplina dei singoli capi, imponendo, caso per caso, una ricognizione di quanto rimasto e un'attenta operazione di coordinamento con le fonti europee.

Chiaramente non sono mancate osservazioni particolarmente critiche rispetto all'operato del legislatore. Permettendo infatti la possibilità di integrare la normativa europea a livello nazionale, l'intento del regolamento, chiaramente, è quello di ottenere regole più chiare, facili da capire e da applicare: un obiettivo che rende ancor più chiara l'evidente paradossalità della situazione italiana. Il testo modificato del d.lgs. 196/2003 in definitiva risulta particolarmente ostico, di difficile comprensione per gli operatori che hanno già familiarità con la disciplina.

Individuare delle coordinate per analizzare in modo compiuto la normativa *de residuo* chiaramente va oltre le possibilità e gli obbiettivi di questo lavoro. Quel che però si può osservare, anche guardando indietro all'*iter* che ha segnato l'evoluzione di questa disciplina, è che nella situazione attuale il quadro normativo che si presenta al termine di queste modifiche è quanto mai complesso. Come rilevano alcuni, dopo il d.lgs. 101/2018, l'impianto del Codice Privacy sia stato smantellato, passando da una disciplina sistematica ad una serie di previsioni affastellate che, in tutto o in parte, sono destinate a rifarsi ora alla disciplina europea, ora agli interventi regolatori del Garante.

### *4.4. Le implicazioni costituzionali del diritto alla protezione dei dati personali*

Alla luce delle considerazioni su esposte, dunque, c'è da chiedersi cosa possa dire oggi il diritto nazionale – costituzionale e non – rispetto alla protezione dei dati personali al tempo dei *big data*. In risposta a questa domanda, forse, possono tornare utili i contributi con cui la dottrina italiana, nel tempo, ha contribuito a mettere in luce le molteplici implicazioni costituzionali di questa disciplina.

Pur riconoscendo un forte legame tra i concetti di riservatezza, autonomia e autodeterminazione informativa, la dottrina italiana fin dall'inizio ha messo a fuoco le differenze che intercorrono tra queste diverse figure giuridiche. Ragionando

soprattutto sui profili legati all'utilizzo delle informazioni, infatti, si è osservato come lo sviluppo delle nuove tecnologie ponga di fronte ad un quadro ambivalente, in cui i benefici organizzativi possono coesistere con nuove derive autoritarie e di controllo.

Come ricordato, le prime riflessioni erano concentrate soprattutto sulla necessità di affermare nuove forme di sovranità individuale e sociale sull'utilizzo delle informazioni, con l'intento di elaborare nuovi meccanismi di trasparenza legati soprattutto alla necessità di consenso e agli strumenti di accesso.

Analizzando il problema in termini più pratici, tuttavia, la prima questione da risolvere concerne sempre la qualificazione di questo genere di attività. Di fronte ad un fenomeno nuovo come quello della digitalizzazione, ci si è chiesti, cioè, dove collocare le aspettative legate all'uso dei computer e all'utilizzo dei dati nel panorama dei diritti costituzionalmente tutelati al fine di individuare i relativi limiti[166].

Com'è noto, pur mancando dei riferimenti normativi puntuali, fin da principio si erano intuiti gli indubitabili vantaggi di questi sistemi, ormai indispensabili per la gestione dei normali flussi informativi attorno cui gravita praticamente ogni attività economico-sociale[167].

Alla luce di queste considerazioni, la dottrina si è così dimostrata concorde nell'affermare che l'utilizzo dei computer, e con esso il trattamento dei dati personali, in linea di principio sia di per sé un'attività lecita e rappresenti una fisiologica estrinsecazione di diversi principi e libertà tutelate dalla Carta costituzionale.

---

166 V. ZENO ZENCOVICH, *Telematica e diritto all'identità personale,* in *Politica del diritto*, 1983, p. 345; G. BUTTARELLI, *Banche dati e tutela della riservatezza,* cit., pp. 81 ss.; G. RESTA, *Il diritto alla protezione dei dati personali*, in F. CARDARELLI, S. SICA, V. ZENO ZENCOVICH (a cura di), *Il codice dei dati personali: temi e problemi*, Milano, Giuffrè, 2004, pp. 19-22; S. NIGER, *Le nuove dimensioni della privacy*, cit., pp. 107 ss.

167 Di quest'avviso, basti ricordare le considerazioni proposte da Stefano Rodotà nel corso della sua opera. *Ex multis*, ID., *Elaboratori elettronici e controllo sociale*, cit. pp. 9 ss.; ID., *Tecnopolitica*, cit., *passim*; ID., *Tecnologie e diritto*, cit., pp. 52 ss.; Id., *Data protection as a fundamental right*, in S. GUTWIRTH et al. (a cura di), *Reinventing Data Protection*?, Springer, 2009, pp. 77ss.

Così come si sono evolute le tecnologie, nel tempo si sono approfondite anche queste riflessioni, tant'è che ad una rapida analisi si scorgono essenzialmente tre principali punti di riferimento.

Innanzitutto si è osservato, come queste attività trovino un primo fondamento costituzionale in quanto previsto dall'art. 21, comma 1 Cost. Specificando come la libertà di manifestazione del pensiero trovi tutela non solo rispetto ai mezzi tradizionali, come la parola o lo scritto, ma copra anche «ogni altro mezzo di diffusione», il testo costituzionale, infatti, astrattamente permette di includere anche la banche dati e le comunicazioni telematiche, così come i loro successivi sviluppi in rete e sui *social media*[168].

Parimenti, guardando a come le risorse informatiche siano divenute in poco tempo una componente imprescindibile in diversi settori dell'economia (non solo nell'ambito della gestione aziendale ma proprio anche come ramo centrale di alcune attività di impresa) si è sottolineato come la raccolta e l'utilizzo dei dati personali possa trovare tutela anche nell'ambito delle libertà legate all'iniziativa economica (art. 41 Cost.)[169].

Infine, non si possono trascurare i vantaggi che l'utilizzo dell'informatica e delle nuove tecnologie *data-intensive* possono portare nell'ambito delle attività della

---

[168] Sui profili abilitanti l'utilizzo dell'informatica e le contrapposte aspettative alla tutela dei dati personali: M. OROFINO, *La libertà di espressione tra Costituzione e Carte europee dei diritti*, cit.; M. OROFINO, *Trattamento dei dati personali e libertà di espressione e informazione*, in L. CALIFANO, C. COLAPIETRA (a cura di), *Innovazione tecnologica e valore della persona*, cit., pp. 509 ss., spec. 516. Altre considerazioni più legate all'attività giornalistica in A. PALMIERI, *Trattamento dei dati personali e giornalismo: alla ricerca di un equilibrio stabile*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, II, Milano, Giuffrè, 2003.

[169] Per avere un'idea chiara basti pensare al consolidarsi di realtà imprenditoriali come Facebook, Google, Amazon e alle collaborazioni che queste grandi aziende instaurano con operatori meno noti, come messo in luce dalle vicende legate al caso Cambridge Analytica. Sull'idea di dato personale come "merce", per tutti S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, cit. pp. 9 ss.; ID., *Tecnologie e diritto*, cit., pp. 52 ss. Per un approfondimento, poi, sulle attività di *data brokering,* in cui il *core business* delle diverse imprese consiste proprio nel mercato dei dati, *ex multis,* Federal Trade Commission (USA), *Data Brokers – A call for transparency and accountability*, maggio 2014, spec. pp. 19 ss.; ID., *Big Data. A tool for Inclusion or Exclusion? Understanding the Issues,* gennaio 2016, spec. pp. 12 ss.; Commissione europea, *Eurpean Data Market Study*, 2° rapporto, 20 marzo 2019.

pubblica amministrazione. Una gestione più efficiente dei flussi informativi, delle banche dati e, in generale, dell'attività conoscitiva e decisionale, infatti, quanto meno in astratto, costituisce un significativo contributo all'efficienza e al buon andamento della pubblica amministrazione (art. 97 Cost) realizzando gli obiettivi costituzionale con nuovi supplementi tecnologici[170].

Con il tempo, però, oltre a questi riferimenti stabili, sono stati poi considerati altri importanti parametri, che grazie alla digitalizzazione oggi presentano implicazioni più o meno dirette rispetto alla *data protection*. In un primo momento, si sono approfondite soprattutto le implicazioni relative al mondo del lavoro, analizzando i benefici che possono derivare dall'utilizzo di queste tecnologie per la realizzazione degli obiettivi economici del datore di lavoro (art. 41 Cost.) e, per contro, le conseguenze di questa rivoluzione tecnologica sull'autonomia e la dignità del lavoratore (artt. 4 e 36 Cost.)[171].

A questi rilievi si aggiungono le profonde riflessioni relative all'utilizzo dei dati e delle nuove tecnologie in ambito penalistico, nel tentativo di trovare il giusto punto di equilibrio tra le esigenze investigative e l'esercizio dell'azione penale nell'interesse della collettività e le legittime aspettative individuali alla segretezza

---

[170] M. LOSANO, *Il diritto pubblico nell'informatica,* Torino, Einaudi, 1986; S. FOA, *Il trattamento dei dati personali per finalità di rilevante interesse pubblico*, in G. SANTANIELLO (diretto da), *Trattato di diritto amministrativo*, Vol. XXXVI, *La protezione dei dati personali*, Padova, Cedam, 2005, pp. 343 ss.; M. FALCONE, *"Big data" e pubbliche amministrazioni. Nuove prospettive per la funzione conoscitiva pubblica*, in *Rivista trimestrale di diritto pubblico,* 3, 2017, pp. 601 ss; S. TOSCHEI, *I trattamenti in ambito pubblico nell'era della digitalizzazione e della trasparenza*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., pp. 397 ss.

[171] Considerazioni già ampiamente emerse con riferimento alle prime norme sulla protezione dei dati personali nel testo dello Statuto dei lavoratori. All'utilizzo di queste tecnologie, tuttavia, oggi si lega la possibilità di attuare nuove misure di flessibilità, attraverso diversi modelli di c.d. *smart working*; potenzialità che hanno messo in luce nuovi benefici e nuovi insidie rispetto a questioni assai delicate. Rispetto all'utilizzo dei dati personali nell'ambito dei rapporti di lavoro, *ex multis,* S. NIGER, *Le nuove dimensioni della privacy,* cit., pp. 176 ss.; C. COLAPIETRO, *Tutela della dignità e riservatezza del lavoratore nell'uso delle tecnologie dei digitali per finalità di lavoro,* in *Giornale di diritto del lavoro e delle relazioni industriali,* 2017, pp. 439 ss.; E. CAPALDO, *Riservatezza, vita privata e tutela della dignità del lavoratore "agile"*, in *Giustiziacivile.com*, 2018.

delle comunicazioni e ad un effettivo godimento dei rimedi giurisdizionali (artt. 15 e 24 Cost.).

Non sono passate inosservate nemmeno le questioni inerenti lo sfruttamento dei dati personali nell'ambito delle attività di studio e ricerca, così come per lo sviluppo della cultura; un tema che, in prospettiva, promette risvolti particolarmente sensibili, soprattutto per quanto riguarda la libertà di ricerca, così come l'accesso all'informazione e all'istruzione (art. 9 e 34 Cost.)[172].

Non ultimi, sono stati approfonditi anche i profili relativi all'utilizzo delle ICT come strumento abilitante la partecipazione sociale, qui nell'ottica di promuovere la comunicazione istituzionale e la collaborazione tra cittadini e amministrazione, attraverso la rete e gli *open data* (artt. 1, 21, 97 Cost.)[173].

Quelle appena accennate sono riflessioni che guardano allo sviluppo delle tecnologie in chiave evolutiva, includendovi anche i fenomeni e le evoluzioni più recenti e quelli che, ipoteticamente, si prospettano in base all'attuale stato dell'arte. Non si può trascurare, tuttavia, la ragione primaria che ha spinto verso questi

---

[172] Alcuni spunti rispetto al potenziale abilitante delle tecnologie informatiche nell'ambito dell'apprendimento in F.M. DE TULLIO, *La privacy e i big data verso una dimensione costituzionale collettiva*, in *Politica del diritto,* 4, 2016, p. 643; V. MAYER-SCHÖNBERGER, K. CUCKIER, *Learning with Big Data: The Future of education,* Boston, Houghton Mifflin Harcourt, 2014. Rispetto invece ai rischi legati alla protezione dei dati personali e al rischio di pratiche discriminatorie, alcune riflessioni in C. MUÑOZ, M. SMITH, D. PATIL, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, The White House, Executive Office of the President, maggio 2016, pp. 16 ss. e, da ultimo, per una sintesi sulle evoluzioni del quadro normativo europeo, E. LONGO, *I trattamenti nel settore dell'istruzione e a fini di ricerca (scientifica, storica, statistica,* in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., pp. 491 ss.

[173] Nella letteratura più recenti, spiccano i temi relativi soprattutto agli *open data* e alle applicazioni di intelligenza artificiale. Per un approfondimento generale si rinvia, *ex multis,* a C. COLAPIETRO E A. IANNUZZI*, Il cammino della trasparenza in Italia: una prospettiva di partecipazione e legittimazione*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Napoli, Editoriale Scientifica, 2014, pp. 117 ss.; M. VIGGIANO, *I limiti alla pubblicità dell'azione amministrativa per finalità d trasparenza derivanti dalla protezione dei dati personali, ibidem*, pp. 216 ss.; C. ROMANO, *Open data* e riutilizzo nel decreto trasparenza: propulsore per la democrazia e lo sviluppo o sfida ulteriore per i diritti fondamentali?, *ibidem*, pp. 263 ss.; M. OREFICE, *Gli open data tra principio e azione: lo stato di avanzamento*, in *Forum di Quaderni Costituzionali,* 2015. Da ultimo, sui profili relativi all'intelligenza artificiale, si rinvia al rapporto dell'Agenzia per l'Italia digitale, *L'intelligenza artificiale al servizio del cittadino: sfide e opportunità*, marzo 2018.

approfondimenti, ossia l'esigenza di individuare dei limiti all'utilizzo dell'informatica e dei dati per dare risposta a problemi primigeni legati all'originaria mancanza di una disciplina.

In retrospettiva, guardando allo sviluppo della normativa, si osserva come, nel settore pubblico l'utilizzo dei dati personali sia sempre stato comunque regolamentato con dei puntuali interventi normativi, legati essenzialmente alla natura amministrativistica dell'attività di trattamento. In questi contesti, il fondamento costituzionale della disciplina emerge implicitamente con l'individuazione di un interesse pubblico meritevole di tutela, rispetto al quale il legislatore individua precisi limiti e criteri di bilanciamento con le diverse aspettative in capo ai soggetti interessati.

Nel settore privato, invece, soprattutto prima della legge n. 675/1996 non era possibile rinvenire agilmente simili coordinate. Sebbene l'art. 41, comma 2 Cost. stabilisca che l'iniziativa economica non può svolgersi in modo tale da arrecare danno alla dignità della persona – così ammettendo che questa libertà possa incontrare dei limiti ed essere regolamentata da specifiche prescrizioni – le uniche norme che fino a quel momento avrebbero potuto permettere una qualche forma di controllo sull'attività dei privati sono state per lungo tempo trascurate[174], lasciando così che l'intero settore delle banche dati si sviluppasse in assenza di una qualche forma di regolamentazione.

È proprio a motivo di queste lacune che si sono quindi cominciati ad approfondire in chiave sistematica i principi costituzionali che possono offrire adeguata tutela alle persone rispetto all'utilizzo delle informazioni che le riguardano. Ed è nell'alveo di queste riflessioni che la protezione dei dati personali è stata

[174] Il riferimento cui si sarebbe potuto rifarsi è ai contenuti degli artt. 115 e 134 del testo unico sulle leggi di pubblica sicurezza (r.d. 18 giugno 1931, n. 773) circa le autorizzazioni agli enti e ai privati che raccolgono informazioni a scopo di divulgativo o investigativo per conto di altri privati. Cfr. G. BUTTARELLI, *Banche dati e tutela della riservatezza*, cit., pp. 83-84.

analizzata in una prospettiva più ampia, affrontando la problematica dei diritti della persona *tout court*.

In tal senso, alcune prime osservazioni sono già state anticipate poc'anzi, analizzando gli ambiti in cui l'utilizzo dell'informatica – seppur legittimo – si scontra con gli interessi di coloro che, in ultima, sono oggetto dell'attività di trattamento. Quel che qui preme evidenziare è come la discussione in quest'ambito si sia concentrata soprattutto sulla natura e sul potenziale espansivo dei diritti della personalità, vagliando la possibilità di delineare un'ulteriore figura di tutela, diversa rispetto a quanto previsto a favore delle omologhe pretese cui si ricollegano il decoro, la riservatezza, l'identità personale.

Nell'intraprendere questa strada, il punto di riferimento sul piano costituzionale è ancora una volta l'art. 2 Cost, porta di ingresso per il riconoscimento di quei nuovi diritti che in qualche modo possono dirsi impliciti o latenti nel dettato della Carta.

In tal senso, ovviamente, le riflessioni circa questi aspetti si sovrappongono in più parti a quanto elaborato a tutela della sfera privata, qui intesa soprattutto come garanzia di riservatezza delle informazioni personali

La dottrina si è confrontata soprattutto sul potenziale espansivo di questa disposizione, ossia se il riferimento ai diritti inviolabili vada letto come una clausola aperta – protesa a garantire la copertura costituzionale agli interessi che via via emergono rispetto allo sviluppo di nuovi fenomeni sociali, economici, tecnologici – oppure se vada interpretata in termini più restrittivi, come una sorta di preludio generale alla catalogazione dei diritti proposti nella prima parte della Carta. Gradualmente, tra queste due diverse istanze, si è fatta strada una terza via che tende a mediare rispetto ai due estremi. L'art. 2 Cost., cioè, ammetterebbe la tutela di nuovi diritti nel momento in cui questi risultino essere impliciti, strumentali o conseguenti rispetto ai diritti originariamente sanciti dalla Carta, interpretati

chiaramente alla luce dei una loro lettura evolutiva ad opera della giurisprudenza di legittimità[175]. di

La protezione dei dati personali, rispetto alle ipotesi sviluppate sulla scia di queste precedenti teorie, secondo alcuni potrebbe trovare un proprio fondamento costituzionale proprio in ragione di questa soluzione intermedia. Tale diritto permette infatti di tutelare proiezioni informative che documentano molteplici

---

[175] Rispetto a queste previsioni e alla loro interpretazione, vanno accennati alcuni profili critici emersi circa la portata di ciascuno. In merito all'art. 2 Cost, non può essere sottaciuto il confronto dottrinale tra l'alternativa di intendere tale previsione come "clausola aperta" o "norma di chiusura". Se, da un lato, secondo alcuni Autori, tale previsione ha lo scopo di individuare i diritti non enumerati secondo il modo in cui emergono attraverso l'ordine naturale, come versione secolarizzata di quest'ultimo, o come costituzione materiale (*ex multis*, A. BARBERA, *Art. 2*, cit., pp. 80 ss.) dall'altro, secondo Altri, un simile approccio circa di ridurre il catalogo previsto dai Costituenti a mera discrezionalità, non senza i rischio di derive soggettivistiche (A. PACE, *Problematiche delle libertà costituzionali. Parte generale*, 3° ed. agg., Padova, Cedam, 2003, pp. 20 ss.). Sulla base di quanto inteso dalla giurisprudenza costituzionale successiva, si è infine optato per una posizione intermedia, leggendo dal riferimento ai diritti inviolabili di cui all'art. 2 Cost. un principio che ammette la protezione di diritti non enumerati, sempre che siano enucleabili a partire da quelli previsti dalla Carta (F. MODUGNO, *I "nuovi" diritti nella giurisprudenza costituzionale*, Torino, Giappichelli, 1995, pp. 2 ss.). Quanto al riferimento alla «pari dignità sociale», soprattutto la dottrina civilistica di quegli anni, ha messo in luce come già nel testo costituzionale si rinvenissero riferimenti che in concreto declinavano il principio in ambiti specifici come, ad esempio, all'art. 36, circa la commisurazione della retribuzione ai fini di un'esistenza libera e dignitosa per lui e la sua famiglia, o all'art. 41, comma 2, ove è menzionata come limite all'esercizio delle libertà economiche; tutte ragioni che hanno indotto a ritenere sue ulteriori possibili declinazioni anche rispetto alla tutela della vita privata (così in S. Niger, *Le nuove dimensioni della privacy*, cit., pp. 46-47). Infine, circa i primi segni di apertura per una lettura ampia dei contenuti dell'art. 13 Cost, comprensiva della libertà morale oltre che della libertà fisica, per tutti, A. BARBERA, *I principi costituzionali della libertà personale*, Milano, Giuffrè, 1967. In tempi più recenti, sempre su questi profili, si rimanda *ex multis*, A. BARBERA, *"Nuovi diritti": attenzione ai confini*, in L. CALIFANO (a cura di), *Corte costituzionale e diritti fondamentali*, Torino, Giappichelli, 2004; C. PICIOCCHI, *I diritti inviolabili*, in C. CASONATO (a cura di), *Lezioni sui principi fondamentali della Costituzione*, Torino, Giappichelli, 2008.

manifestazioni della personalità umana, estendendo così le tradizionali garanzie ad una serie di interessi fondamentali riconducibili a specifici diritti soggettivi.

Alla luce di queste considerazioni, rimane però da capire che natura potrebbe assumere una simile figura giuridica, ossia come si debbano configurare le aspettative dei soggetti sottoposti nelle attività di trattamento dei dati personali e degli interessati cui tali informazioni si riferiscono.

Altre legislazioni hanno chiarito in modo puntuale gli obiettivi e i fini delle proprie normative sulle informazioni personali, richiamando ora il libero sviluppo della personalità, ora alcuni diritti fondamentali specifici come la vita privata, l'intimità della sfera individuale e familiare o l'onore[176]. A differenza di questi esempi, invece, anche sulla scorta di considerazioni di cui sopra, la disciplina italiana, dalla legge del 1996 in poi, si è orientata per una lettura della protezione dei dati in termini più ampi, volta a garantire che il trattamento di questi contenuti avvenga nel rispetto di *tutti* i diritti e le libertà fondamentali. Certo non manca un particolare accento sulla tutela della riservatezza e dell'identità personale (principi richiamati immediatamente dopo questa generale dichiarazione d'intenti). Tuttavia, per la natura stessa della disciplina, questi due diritti sono qui tutelati soltanto per quanto attinente alle loro estrinsecazioni informative, segnando quindi una chiara linea di demarcazione tra le diverse aree coperte dai diversi sistemi di protezione[177].

Quest'inciso è stato letto da molti come un esplicito ancoraggio dell'intera disciplina non tanto e non solo all'art. 2, quanto soprattutto al successivo art. 3 Cost, definendo come limite al trattamento dei dati e presupposto del diritto alla loro

---

[176] Si pensi, ad esempio, alla normativa svizzera e francese che sanciscono il valore e la funzione sociale dell'informatica, la quale «non deve attentare né all'identità né ad altri diritti dell'uomo né alla vita privata né alle libertà individuali e pubbliche»; o a quella belga e olandese che prevedono puntualmente uno specifico rapporto tra tutela dei dati e tutela della *privacy*. Circa questi diversi approcci, si rimanda a G. BUTTARELLI, *Banche dati e tutela della riservatezza. La* privacy *nella Società dell'Informazione*, cit. pp. 81-82, nn. 1, 2 e 3; per una ricognizione più recentemente, si veda G. GONZÁLEZ FUSTER, *The emergence of data protection as a fundamental right of EU*, cit., pp. [56-70] e [92-94].

[177] G. Tiberi, *Riservatezza e protezione dei dati personali*, cit., p. 355.

protezione proprio il principio di dignità. Così posto al centro della normativa, tale principio consentirebbe infatti di individuare non solo i limiti ultimi che l'agire della pubblica amministrazione incontra anche nei provvedimenti di natura più compromissoria della libertà personale[178], ma anche una delle condizioni essenziali all'esercizio dell'iniziativa economica e all'attività di impresa[179].

La protezione dei dati personali, dunque, pur costituendo oggi un diritto fondamentale concettualmente autonomo da altri, rappresenta un insieme di garanzie procedurali volte a garantire nei singoli casi la tutela degli interessi sostanziali legati al trattamento delle informazioni, bilanciando così le legittime aspettative del titolare e, per contro, le prerogative dell'interessato al rispetto della sua libertà e della dignità della sua persona. È soltanto alla luce di queste premesse che trovano ragione, da un lato, la dimensione istituzionale di questo diritto, e così i complessi meccanismi di tutela che ne regolano la disciplina e ne assicurano l'effettiva protezione (basti pensare al ruolo e ai poteri in capo all'Autorità garante). Dall'altro, invece, questo rappresenta un esempio solare nella nuova ecologia giuridica che informa la tutela dei diritti fondamentali, in cui la protezione dei dati personali si connota come un complesso di misure che implicano rilevantissimi costi, pubblici e privati, e tutto ciò a prescindere dalle tradizionali distinzioni tra diritti di libertà e diritti sociali[180].

---

[178] Basti pensare a quanto previsto dall'art. 32, comma 2, Cost., con riferimento ai trattamenti sanitari obbligatori, quanto si legge che «La legge non può in nessun caso violare i limiti imposti dal rispetto della persona umana» e dall'art. 27, comma 3, Cost., quando con riferimento alle pene si richiama «Le pene non possono consistere in trattamenti contrari al senso di umanità e devono tendere alla rieducazione del condannato».

[179] I riferimenti vanno ovviamente all'art. 41, comma 2, Cost., in merito ai già ricordati limiti per cui l'attività economica «Non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana».

[180] M. CARTABIA, *Le norme sulla privacy come osservatorio sulle tendenze attuali delle fonti del diritto*, in M. LOSANO (a cura di), *La legge italiana sulla* privacy, cit., p. 68, riferendosi in particolare alle riflessioni elaborate in C.R. SUSTEIN, *Il costo dei diritti*, Bologna, Il Mulino, 2000.

Le considerazioni fin qui esposte, senz'altro valide agli albori di questa disciplina, si confermano di vitale importanza anche oggi per affrontare le questioni che oggi si prospettano con lo sviluppo dei *big data*.

Guardando a questo fenomeno tecnologico sono state utilizzate diverse metafore per descriverlo, dalle inondazioni alle esplosioni[181]; metafore che, pur semplificando, consentono di cogliere la portata della trasformazione in corso. Sebbene infatti già si intuisse che il destino delle ICT avrebbe portato a questo punto[182], soltanto ora si comincia a toccare con mano come la c.d. società dell'informazione navighi in un'immensa quantità di contenuti cui, quotidianamente, in ogni istante, continuano ad aggiungersene di nuovi, aumentando in termini esponenziali.

Per quel che riguarda la protezione dei dati personali, questi sviluppi hanno messo in forte crisi la tradizionale architettura della disciplina. In una realtà datificata, capire che cosa costituisca effettivamente un "dato personale" risulta già un'impresa complessa: non si tratta più, infatti, solo delle informazioni identificative che provengono dal soggetto ma anche di tutti quei contenuti che, attraverso operazioni sempre più complesse, possono essergli in qualche modo attribuite[183].

---

[181] L. FLORIDI, *La rivoluzione dell'informazione*, Torino, Codice Edizioni, 2012, p. 7. (sul concetto di *exaflood*, poi ripreso anche in L. FLORIDI, *Quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, Cortina Editore, 2017); D.E. HOLMES, *Big Data. A very short introduction*, Cambridge, Cambridge University Press, 2014, pp. 1 ss. (sull'idea di esplosione).

[182] Basti pensare alle preoccupazione emerse a suo tempo da parte di diversi autori. Cfr. S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, cit. p. 17(sindrome dell'elaboratore); K.C. LAUDON, *Dossier Society: Value Choices in the Design of National Information Systems*, New York, Columbia University Press, 1986, (società dei dossier); V. PACKARD, *The Naked Society*, Harmondsworth, Penguin Books, 1971 (edizione originale: 1964) (cittadino trasparente); S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove forme di comunicazione*, Laterza, Roma-Bari, 2004 (tecnopolitica); F. PASQUALE, *The Black Box Society*, *The Secret Algorithms That Control Money and Information*, Cambridge,

[183] Si vadano in tal senso i pareri del Gruppo Articolo 29 a chiarimento dei concetti di dato personale e sulle tecniche di anonimizzazione, rispettivamente: *Parere 4/2007 sul concetto di dato personale*, 20 giugno 2007 (WP136); *Parere 05/2014 sulle tecniche di anonimizzazione*, 10 aprile 2014 (WP216). In dottrina, rispetto alle criticità incontrate in quest'ambito si rinvia, *ex multis*, a N. PURTOVA, *The law of everything. Broad concept of personal data and future of EU data protection law*, in *Law, Innovation and Technology*, 2018, pp. 40 ss.

Soprattutto guardando ai principi fondamentali di questa disciplina, si è osservato come altri meccanismi siano messi a dura prova dallo sviluppo di un'economia *data-intensive*. Il principio di finalità del trattamento, ad esempio – così come i meccanismi che si basano sulla logica del consenso – in un sistema in cui gli elementi possono essere elaborati e rielaborati, aggregati e scomposti più e più volte sembra entrare definitivamente in crisi, a meno che non si voglia ridurre a meri formalismi[184].

Allo stesso modo, sulla protezione dei dati e dei diritti dell'interessato, incidono in modo evidente l'architettura stessa dei sistemi utilizzati, e così le misure tecnico-organizzative pensate per controllare la regolarità dei processi. In tal senso, dunque, risulta determinante prendere posizione anche rispetto a questi aspetti, decidendo se e come promuovere lo sviluppo di tecnologie e procedure allineate ai valori sociali e quali diritti assicurare oggi all'interessato per far valere i propri interessi circa l'utilizzo dei suoi *big personal data*[185].

Le considerazioni appena accennate vogliono offrire soltanto alcuni spunti, anticipando temi e riflessioni che saranno approfondite meglio nel capito seguente, analizzando la disciplina del GDPR.

---

[184] Sempre con riferimento al principio di finalità, si vedano i lavori del WP29, *Opinion 03/2013 on purpose limitation*, 2 aprile 2013 (WP203); *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*, 16 settembre 2014 (WP221). A commento sul tema, *ex multis*, A. Mantelero, *La privacy all'epoca dei big data*, in V. CUFFARO, R. D'ORAZIONE, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., pp. 1192 ss.; F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento dei dati personali*, in G. FINOCCHIARO (diretto da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, pp. 124 ss.

[185] Rispetto al valore di queste misure, oltre alle prossime indicazioni del Garante europeo (EDPS, *Opinion 5/2018 – Preliminary Opinion on privacy by design,* 31 maggio 2018), si vedano, *ex multis*, G. D'ACQUISTO, M. NALDI, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, Giappichelli, 2017 (capitolo 1); S. CALZOLAIO et al, *La responsabilità e la sicurezza del trattamento*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., pp. 170 ss.; F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. CUFFARO, R. D'ORAZIONE, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., pp. 793 ss. e 814 ss.; R. TORINO, *La valutazione di impatto (Data Protection Impact Assessment)*, *ibidem,* pp. 855 ss.,; A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione di impatto e consultazione preventiva*, in G. FINOCCHIARO (diretto da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., pp. 310 ss.

La struttura del catalogo dei diritti come ampliata dal regolamento, così come le nuove misure di tutela previste per i processi esposti a più gravi rischi, certo documentano una mutata sensibilità rispetto a questi profili legati alle innovazioni che stanno prendendo piede. La previsione di più solide garanzie a favore del diritto di accesso, così come l'implicita previsione di un diritto ad una spiegazione nell'ambito dei processi di decisione automatizzata, sono radicate nella convinzione che anche in questo nuovo ecosistema informativo debbano trovare tutela valori fondamentali come il principio di trasparenza e il diritto di difesa.

Allo stesso modo, prendendo in esame la disciplina relativa alle misure *by design* e *by default*, così come gli obblighi in materia di valutazione di impatto, si trovano ulteriormente rafforzati i profili oggettivi e istituzionali della disciplina, ponendo in capo, trasversalmente, a tutti gli attori coinvolti nell'attività di trattamento, un generale dovere di cura (*duty of care*) dei diritti fondamentali delle persone coinvolte.

Avendo a mente queste sfide alla tutela dei diritti fondamentali di fronte ai *big data*, si andranno ad approfondire i tratti del diritto fondamentale alla protezione dei dati personali *ex* art. 8 CDFUE, ricostruendone le origini nel contesto europeo fino ad oggi per scorgere come questo si innesti nel precedente tessuto costituzionale nazionale e comunitario.

## 5. La protezione dei dati personali in un sistema di tutele multilivello: quali prospettive?

Il motivo per cui si è insistito tanto su queste premesse sullo stato dell'arte in materia di *privacy* e *data protection* nell'ordinamento interno è soprattutto uno. Nel corso degli ultimi anni, infatti, la Corte costituzionale, pur non essendosi occupata precipuamente di tali temi, con alcune sue pronunce ha preso posizioni nette sui

rapporti tra il diritto interno e il sistema europeo, soprattutto per quanto concerne la tutela dei diritti fondamentali[186].

Tradizionalmente, la Consulta ha tenuto dei rapporti particolarmente algidi nei confronti della Corte di Giustizia EU, prima facendo resistenza nel proporre essa stessa dei rinvii pregiudiziali a Lussemburgo, poi, in generale, lasciando comunque quest'incombenza alla discrezionalità dei giudici ordinari. In virtù di tale prassi, dunque, si spiega perché molto spesso i magistrati nazionali, quando si siano trovati ad avere dubbi sulla compatibilità tra diritto italiano e diritto comunitario, abbiano preferito rivolgersi ai colleghi lussemburghesi; e questo anche quando venissero a tema diritti tutelati tanto dalla nostra Carta fondamentale, quando dalla Carta di Nizza.

A fronte di questa "devianza indotta", in parte anche dalla precedente giurisprudenza costituzionale, il Giudice delle leggi, in tempi recenti ha ravvisato l'opportunità di riaffermare le proprie prerogative, intervenendo a ridefinire in modo energico (seppur non sempre cristallino) l'equilibrio dei rapporti con la CGUE.

Questo *revirement* ha subito attratto una lunga serie di interventi e commenti, volti a decifrare e a chiarire di volta in volta il significato puntuale dei singoli passaggi argomentativi sviluppati dalla Corte. Per un approfondimento di portata generale, si rinvia quindi a questa vasta produzione[187]. Quello che qui preme

---

[186] Corte cost. sentt. nn. 679/2017, 115/2018, 63/2019.

[187] *Ex multis,* A. BERNARDI (a cura di), *I controlimiti. Primato delle norme europee e difesa dei principi costituzionali*, Napoli, Jovene, 2017, in particolare i saggi di A. RUGGERI, *Primato del diritto sovranazionale versus identità costituzionale? (Alla ricerca dell'araba fenice costituzionale: i «controlimiti»)*, ivi, p. 19 ss.; E. CANNIZZARO, *Sistemi concorrenti di tutela dei diritti fondamentali e controlimiti costituzionali*, ivi, p. 45 ss.; M. LUCIANI, *Il brusco risveglio. I controlimiti e la fine mancata della storia costituzionale*, ivi, p. 63 ss.; R. BIN, *Taricco, una sentenza sbagliata: come venirne fuori?*, ivi, p. 291 ss.; O. CHESSA, *Meglio tardi che mai. La dogmatica dei controlimiti e il caso Taricco*, ivi, p. 301 ss. C. CARUSO, *La Corte costituzionale riprende il cammino comunitario: invito alla discussione sulla sentenza n. 269 del 2017*, in *Forum di Quaderni Costituzionali*, 18 dicembre 2017; S. VERNUCCIO, *La sentenza 269/2017: la Corte costituzionale di fronte alla questione dell'efficacia diretta della Carta di Nizza e la prima risposta del giudice comune (Cass. ord. 3831/2018)*, in *Osservatorio Costituzionale*, n. 2/2018, p. 2.; G. SCACCIA, *Giudici comuni e diritto*

mettere in luce, invece, è proprio il fatto che, in quest'operazione di ridefinizione dei confini, la giurisprudenza costituzionale ha colto l'occasione per affrontare i problemi che si incontrano su questi versanti quanto alla disciplina sulla protezione dei dati personali[188].

Preso atto delle «trasformazioni che hanno riguardato il diritto dell'Unione e il sistema dei rapporti con gli ordinamenti nazionale dopo l'entrata i vigore del Trattato di Lisbona […] che, tra l'altro, ha attribuito effetti giuridici vincolanti alla Carta dei diritti fondamentali dell'Unione europea», la Corte non ha mancato di evidenziare come i principi e i diritti enunciati a Nizza intersecano in larga misura i principi e diritti garantiti dalla Costituzione italiana (così come dalle altre Costituzioni nazionali degli Stati membri). Si è quindi sottolineato come il *bill of rights* europeo rappresenti una «parte del diritto dell'Unione dotata di caratteri peculiari [proprio] in ragione del suo contenuti di impronta tipicamente costituzionale»[189].

Cionondimeno, ribandendo la centralità del proprio scrutinio in materia, la Consulta ha anche sottolineato come, fermi restando i principi del primato e dell'effetto diretto del diritto comunitario, in ogni caso «occorre considerare le peculiarità delle situazioni nelle quali, in un ambito di rilevanza comunitaria, una legge che incide sui diritti fondamentali della persona sia oggetto di dubbi» e questo «sia sotto il profilo della sua conformità alla Costituzione, sia sotto il profilo della sua compatibilità con la CDFUE»[190].

Già in precedenza, a riguardo, il Giudici delle leggi avevano avuto modo di chiarire come nei casi di c.d. doppia pregiudizialità – ossia le situazioni in cui «la violazione di un diritto della persona infranga, ad un tempo, sia le garanzie presidiate

---

*dell'Unione europea nella sentenza della Corte costituzionale n. 269 del 2017*, in *Giurisprudenza costituzionale*., n. 6/2017, p. 2948.

[188] Corte cost. sent. n. 20/2019.

[189] Corte cost., sent. n. 679/2017, *Considerato in diritto*, § 5.2, secondo capoverso.

[190] Corte cost., sent. n. 20/2019, *Considerato in diritto*, § 2.1, primo capoverso.

dalla Costituzione italiana, sia quelle codificate dalla Carta dei diritti dell'Unione»[191] – non si possa dare per scontata l'immediata preminenza del rinvio pregiudiziale comunitario. Anzi. Caso per caso, il giudice ordinario dovrà necessariamente sollevare «la questione di legittimità costituzionale, fatto salvo il ricorso al rinvio pregiudiziale per le questioni di interpretazione o di invalidità del diritto dell'Unione»[192].

Si tratta chiaramente di un cambio di rotta che ha qualcosa di epocale[193], soprattutto se si considera lo *status quo ante*, alla luce dei criteri sanciti ormai storicamente dalla sentenza *Granital*[194], nel 1984. A questo poi si aggiunge il fatto che, se il giudice *a quo* solleva la questione di legittimità con riferimento a norme europee che violano un diritto tutelato sia dalla Costituzione, sia dalla Carta, il Giudice delle leggi deciderà prima di tutto «alla luce dei parametri interni» e, solo eventualmente e in seconda battuta alla luce dei riferimenti comunitari[195], «secondo l'ordine di volta in volta appropriato anche al fine di assicurare che i diritti garantiti dalla [Carta di Nizza] siano interpretati in armonia con le tradizioni costituzionali»[196].

---

[191] Corte cost., sent. n. 679/2017, *Considerato in diritto*, § 5.2, secondo capoverso.

[192] Corte cost., sent. n. 679/2017, *Considerato in diritto*, § 5.2; sent. n. 20/2019, *Considerato in diritto*, § 2.1.

[193] S. VERNUCCIO, *La sentenza 269/2017*, cit., p. 2.

[194] Corte cost., sent. 170/1984.

[195] F. SALMONI, *Controlimiti, diritti con lo stesso* nomen *e ruolo accentrato della Consulta. L'integrazione del parametro con le fonti europee di diritto derivato e il sindacato sulla "conformità" alla Costituzione e la mera "compatibilità" con la Carta dei diritti fondamentali dell'UE*, in *Federalismi.it,* 17 aprile 2019, n. 8/2019, p. 9; G. SCACCIA, *L'inversione della "doppia pregiudizialità" nella sentenza della Corte costituzionale n. 269 del 2017: presupposti teorici e problemi applicativi*, in *Forum di Quaderni Costituzionali*, 25 gennaio 2018, p. 3.

[196] È bene notare, peraltro, come si siano orientate in tal senso anche altre Corti costituzionali nazionali. Come osservato dalla Consulta medesima, « In senso analogo, del resto, si sono orientate altre Corti costituzionali nazionali di antica tradizione (si veda ad esempio Corte costituzionale austriaca, sentenza 14 marzo 2012, U 466/11-18; U 1836/11-13)» (rif. Corte cost., sent. n. 679/2017, *Considerato in diritto*, § 5.2). Si veda anche: R. ROMBOLI, *Dalla «diffusione» all'«accentramento»: una significativa linea di tendenza della più recente giurisprudenza costituzionale*, in *Foro Italiano*, n. 143/2018, pp. 22226 ss.

Affrontando dunque le questioni di legittimità che erano emerse circa quanto previsto del c.d. Decreto Trasparenza[197], la Consulta ha chiarito la portata di questi assunti per ciò che concerne il diritto alla protezione dei dati personali, tracciando utili coordinate per cogliere il rapporto tra quanto previsto dal dettato costituzionale e quanto sancito, invece, dall'art. 8 CDFUE.

Nello specifico, al centro della vicenda, vi erano gli obblighi di pubblicazione imposti alle pubbliche amministrazioni per rendere chiari i compensi e le altre utilità percepite da tutti i dirigenti pubblici nell'adempimento del loro servizio (con e senza incarichi politici) [198]. Chiaramente, la divulgazione di simili informazioni – coinvolgendo peraltro tutta la categoria indicata, senza alcuna distinzione – poteva porre qualche problema circa il rispetto dei diritti sanciti dall'art. 7 e 8 CDFUE, così come alle analoghe prerogative che nel nostro ordinamento ottengono copertura costituzionale. Cionondimeno, il TAR rimettente àncora le proprie censure non solo all'art. 117, primo comma, Cost. – così richiamando quanto previsto dalla Carta di Nizza (artt. 7, 8 e 52) – bensì anche l'art. 3 Cost. – per far valere l'intrinseca irragionevolezza della disciplina – e gli artt. 2 e 13 Cost., così da mettere in luce le

---

[197] Le questioni le legittimità, in particolare, hanno investito l'art. 14, commi 1-*bis* e 1-*ter*, d.lgs. 14 marzo 2013, n. 33, *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni.*

[198] Come si legge, infatti, «in particolare, l'art. 14, comma 1-*bis*, estende a tutti i titolari di incarichi dirigenziali nella pubblica amministrazione, a qualsiasi titolo conferiti, gli obblighi di pubblicazione di una serie di dati, obblighi già previsti dal citato art. 14, comma 1, del d.lgs. n. 33 del 2013 a carico dei titolari di incarichi politici, anche se non di carattere elettivo, di livello statale, regionale e locale. Il rimettente censura la disposizione nella parte in cui stabilisce che le pubbliche amministrazioni pubblichino, per i dirigenti, i compensi di qualsiasi natura connessi all'assunzione della carica, gli importi di viaggi di servizio e missioni pagati con fondi pubblici (art. 14, comma 1, lettera c); le dichiarazioni e attestazioni di cui agli artt. 2, 3 e 4 della legge 5 luglio 1982, n. 441 (Disposizioni per la pubblicità della situazione patrimoniale di titolari di cariche elettive e di cariche direttive di alcuni enti), ovvero la dichiarazione dei redditi soggetti all'imposta sui redditi delle persone fisiche e quella concernente i diritti reali su beni immobili e su beni mobili iscritti in pubblici registri, le azioni di società, le quote di partecipazione a società, anche in relazione al coniuge non separato ed ai parenti entro il secondo grado, ove essi vi acconsentano, dovendosi in ogni caso dare evidenza al mancato consenso (art. 14, comma 1, lettera f)» (rif. Corte cost. sent. n. 20/2019, *Considerato in diritto*, § 1, terzo e quarto capoverso).

implicazioni legate alla divulgazione di dati sensibili e le relative conseguenze sulla *privacy*.

In ragione di questi riferimenti, dunque, la Corte costituzionale, affermata la propria competenza a giudicare del caso[199], come aveva già fatto in precedenza, lascia il passo «ad un criterio assiologico-sostanziale, che attiene alla capacità delle norme d'incarnare i valori fondamentali dell'ordinamento»[200]. Considerato, infatti, come le disposizioni oggetto di censura, pur essendo soggette al diritto europeo, incidano «su principi e diritti fondamentali tutelati dalla Costituzione italiana»[201], contrariamente a quanto ci sarebbe potuti attendere, decide di esprimere il proprio giudizio alla luce dei parametri costituzionali interni. E nel percorrere questa strada, addirittura, decide di adottare una soluzione aperta, «non facendo alcun riferimento ad un qualche diritto in particolare, bensì [rifacendosi *n.d.a.*], più in generale, alla necessaria conformità alla Costituzione e alla compatibilità con la Carta della legge oggetto di giudizio»[202].

Alla luce di queste considerazioni, dunque, per una serie di motivi attinenti l'evoluzione storica della normativa sulla trasparenza, la Corte è giunta a concludere per la parziale fondatezza della questione prospettatale. In particolare, si osserva come, pur «in vista della trasformazione della pubblica amministrazione in una "casa

---

[199] Richiamandosi a quanto deciso dalla CGCE nella sent. 20 maggio 2003, *Österreichischer Rundfunk e altri* (cause riunite C-465/00, C-138/01 e C-139/0120), la Consulta ha osservato, infatti, come «pur avendo ritenuto, a seguito di rinvio pregiudiziale, che gli artt. 6, paragrafo 1, lettera c), e 7, lettere c) ed e), della ricordata direttiva 95/46/CE contengono norme direttamente applicabili – [la giurisprudenza europea] ha stabilito che la valutazione sul corretto bilanciamento tra il diritto alla tutela dei dati personali e quello all'accesso ai dati in possesso delle pubbliche amministrazioni doveva essere rimessa al giudice del rinvio, escludendo perciò che fosse stata definitivamente compiuta dalla normativa europea» (rif. Corte cost. sent. 20/2019, *Considerato in diritto*, § 2, quarto capoverso).

[200] A. RUGGERI, *Svolta della Consulta sulle questioni di diritto eurounitario assiologicamente pregnanti, attratte nell'orbita del sindacato accentrato di costituzionalità, pur se riguardanti norme dell'Unione self-executing (a margine di Corte cost. n. 269 del 2017)*, in *Rivista di Diritti Comparati*, n. 3/2017, p. 6.

[201] Corte cost., sent. 20/2019, *Considerato in diritto*, § 2.3.

[202] F. SALMONI, *Controlimiti, diritti con lo stesso* nomen *e ruolo accentrato della Consulta,* cit. p. 15.

di vetro"»[203], l'onere di pubblicazione previsto dalle norme in esame risulta sproporzionato rispetto alle finalità perseguite[204]. Imporre infatti a tutti i dirigenti, indiscriminatamente, la pubblicazione dei propri dati patrimoniali e reddituali, viola innanzitutto l'art. 3 Cost. sotto il profilo della ragionevolezza intrinseca[205]; e tutto ciò risulta ancor più grave se si considerano le implicazioni ulteriori che una simile divulgazione comporta quando operata con l'utilizzo del *web*[206].

Al netto delle conclusioni rispetto al caso di specie, tuttavia, chi si occupa di diritto costituzionale e nuove tecnologie ha subito colto come queste considerazioni, in prospettiva, possano aprire nuovi punti di dialogo tra l'ordinamento interno e quello comunitario[207]. Come si avrà modo di vedere nei prossimi capitoli, infatti, la tutela dei diritti a livello europeo spesso è condizionata da obiettivi e finalità diverse da quelle per cui tali interessi sono protetti a livello nazionale. E ciò emerge ancor più chiaramente per quanto riguarda la *data protection*, soprattutto per la polivalenza di questa figura, di cui già si è avuto modo di accennare ampliamente.

Alla luce di queste considerazioni, dunque, si andrà ad esaminare come si è evoluto il sistema di tutele in questo settore nel contesto comunitario, onde cogliere poi, in seguito, le aree e i diritti in cui maggiormente si rischiano dei contrasti tra i giudici costituzionali nazionali e la Corte di Lussemburgo quando alla funzione del diritto protezione dei dati personali rispetto allo sviluppo dei *big data*.

---

[203] Corte cost., sent. 20/2019, *Considerato in diritto*, § 5.2.
[204] *Ibidem,* § 5.3.
[205] *Ibidem*, § 5.2, ultimo capoverso.
[206] *Ibidem*, § 5.3.1.
[207] O. POLLICINO, *Not to be Pushed Aside: the Italian Constitutional Court and the European Court of Justice*, in *Verfassungsblog – on matters constitutional*, 27 febbraio 2019 [disponibile a questo link].

# Capitolo 3

## La protezione dei dati personali come diritto fondamentale
*verso un modello di tutela unitario a livello europeo*

### 1. Introduzione

Come osservato, «pochi altri diritti appartenenti alla cosiddetta "nuova generazione" possono vantare l'autentica e solida matrice europea che è propria del diritto alla protezione dei dati personali» [208] e questo trova piena conferma nell'evoluzione della relativa disciplina, fin dalle sue prime origini.

In anni in cui era ancora categoricamente escluso che la Comunità europea potesse vantare una specifica competenza in materia di diritti fondamentali[209], la direttiva 46/95 CE rappresenta infatti forse uno dei primi atti normativi comunitari che, oltre a promuovere le libertà fondamentali del diritto europeo, predispone una specifica regolamentazione per la tutela dei diritti della persona[210].

---

[208] L. CALIFANO, C. COLAPIETRO, *Introduzione*, in ID. (a cura di), *Innovazione tecnologica e valore della persona*, Napoli, Editoriale Scientifica, 2017, p. xxiii.

[209] È proprio in quegli stessi anni che la Corte di Giustizia (CGCE), interpellata sul punto, con il parere n. 2/94 aveva constatato l'assenza di competenze al riguardo dei diritti fondamentali dell'uomo e aveva così precluso la possibilità che la Comunità europea potesse aderire come contraente autonomo alla Convezione europea sui diritti dell'uomo.

[210] P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione europea*, cit., p. 81, con riferimento a quanto affermato, *ex multis*, in F. MACARIO, *La protezione dei dati personali nel diritto privato italiano*, in V. CUFFARO, V. RICCIUTO (a cura di), *La disciplina del trattamento dei dati personali*, Torino, Giappichelli, 1997, p. 5. Si osserva infatti come: «la direttiva si presenta come uno degli atti normativi comunitari più significativi nel dibattito, ormai abbastanza maturo, sulla tutela dei diritti dell'uomo e dei diritti fondamentali nell'ambito del diritto europeo» (p. 14, nota 25).

Come si è già avuto modo di osservare nel capitolo precedente, la disciplina sulla protezione dei dati personali, per sua natura, intercetta molteplici settori e si presta ad incidere in ambiti molto delicati della vita quotidiana delle persone e della collettività. Ed è per questo motivo che, attorno a quanto previsto dalla c.d. "direttiva madre", il quadro normativo si è progressivamente ampliato in altri documenti, specificando e adattando le prescrizioni di carattere più generale alle esigenze dei singoli contesti[211].

Chiaramente la normativa, nel tempo, ha subito importati modifiche, fino ad assumere oggi una fisionomia completamente nuova. Nell'ottica di comprendere meglio i passaggi che hanno segnato queste evoluzioni e le prospettive che si aprono con il reg. 679/2016, l'obiettivo di questo capitolo è quello di ripercorrere l'itinerario svolto dal diritto europeo, analizzando gli sviluppi della disciplina e del quadro istituzionale di riferimento al fine di comprendere il contesto entro cui si sviluppa la nuova strategia di *data governance* europea.

## 2. L'evoluzione della disciplina sulla protezione dei dati personali a livello europeo

Fino all'entrata in vigore del nuovo regolamento generale sulla protezione dei dati personali (reg. 679/2016) la disciplina di questa materia a livello europeo è definita soprattutto in ragione dei principi sanciti dalla dir. 95/46. Come si avrà modo di vedere nelle prossime pagine, in tempi e situazioni profondamente diverse,

[211] Anche nel diritto comunitario, si registrano tratti simili a quelli che hanno caratterizzato gli sviluppi della disciplina in seno al Consiglio d'Europa, in cui, come già ricordato, dopo la Convenzione n. 108/1981, negli anni si sono susseguite una serie di raccomandazioni *ad hoc* per i singoli settori, ad opera del Comitato dei Ministri. Guardando al contesto europeo, un primo tentativo di ricognizione in tal senso, è disponibile in F. PIZZETTI, *Privacy e il diritto europea alla protezione dei dati personali*, vol. II, *Il Regolamento europeo 2016/679*, cit., pp. 14-15.

a questa si sono aggiunte poi una serie di ulteriori normative[212], dando vita ad una prima embrionale strategia di *data governance* europea.

Evidentemente, il più delle volte ci si trova di fronte ad una serie di fonti ordinarie, volte soprattutto ad armonizzare la disciplina di settore alla luce dei valori e dei principi che tradizionalmente ispirano il diritto comunitario (*in primis*, la libertà di circolazione delle merci e dei servizi). Prendendo a riferimento soprattutto le teorie sviluppate sulla protezione dei dati nell'ordinamento di Strasburgo, il legislatore europeo e la Corte di giustizia UE, in questa prima fase, infatti, hanno attinto soprattutto dai parametri Cedu, sviluppando solo con il tempo un vero e proprio approccio comunitario al tema.

Analizzando l'evoluzione della disciplina, dunque, si possono scorgere i punti e le questioni che in principio hanno costituito la linfa di questa materia; snodi in grado di dar conto, in chiave storica, dei problemi che oggi ci si trova ad affrontare con le tecnologie di avanguardia.

Si andranno ad approfondire quindi le premesse allo sviluppo della disciplina europea sulla *data protection*, esaminando brevemente i contenuti delle diverse normative. L'obiettivo è quello di ricostruire il quadro storico, e così l'evoluzione delle figure e dei meccanismi di tutela, verso il pieno ed effettivo riconoscimento del diritto fondamentale alla protezione dei dati personali *ex* art. 8 CDFUE.

### *2.1. Disciplinare la protezione dei dati personali a livello europeo*

Come osservato, l'evoluzione della disciplina sulla protezione dei dati personali può essere studiata a partire da diversi punti di vista, ripartendo l'*iter* storico che ha

[212] Nello specifico, in questo capitolo ci si soffermerà soprattutto sulle novità introdotte dal reg. 2001/45, dalla dir. 2002/58 e dalla dir. 2004/26. Gli interventi in materia, tuttavia, sono ben più estesi poiché in diversi ambiti la disciplina sulla protezione dei dati personali intercetta altre normative. Per una panoramica sul tema si rinvia a F. PIZZETTI, *Privacy e il diritto europea alla protezione dei dati personali*, vol. II, *Il Regolamento europeo 2016/679*, cit..

portato al punto in cui siamo ora guardando al susseguirsi delle tecnologie di nuova generazione[213], ora analizzando gli sviluppi istituzionali e culturali del contesto rispetto cui si ragiona[214].

Chiaramente, si tratta di due prospettive legate da una forte complementarietà, ed è per questo che nel delineare il quadro entro il quale si collocano i diversi tasselli che hanno composto la normativa di questa materia si proverà a tenerle in considerazione entrambe.

Da un punto di vista storico, giova ricordare che se la direttiva «madre» recava la data del 24 ottobre 1995, il percorso verso l'approvazione di una disciplina comunitaria in questo settore era cominciato quasi trent'anni prima, nello stesso periodo in cui tali problemi avevano guadagnato priorità nelle agende nazionali[215].

All'epoca, il tema aveva sollecitato gli interessi delle istituzioni europee essenzialmente per due motivi. Da un lato, pensando allo sviluppo del mercato digitale comunitario, preoccupavano le posizioni di forza conquistate da alcune grandi società informatiche americane[216]. Dall'altro, invece, si guardava con perplessità alla frammentazione del quadro normativo interno. Diversi Stati membri, infatti, aveva elaborato un approccio normativo originale; una condizione che certo

---

[213] V. MAYER-SCHÖNBERGER, *Generational Development of Data Protection in Europe*, in P.E. AGRE, M. ROTENBERG (a cura di), *Technology and Privacy: The New Landscape*, cit., p. 219.

[214] G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection in the EU*, cit.

[215] Per una prima sintesi sui punti di contatto tra disciplina nazionale, documenti internazionali e, tra questi, le prime raccomandazioni a livello comunitario si rinvia a F.W. HONDIUS, *Emerging data protection in Europe*, cit. Il merito di questo scritto, infatti, come chiarisce l'Autore, è quello di fotografare un *work in progress*, negli anni in cui si stava andando a sviluppare, prendendo in esame lo stato di avanzamento dei lavori delle diverse assemblee legislative impegnate sui temi della protezione dei dati personali in Europa e le ricerche svolte a livello sovranazionale nell'elaborazione dei primi documenti su questo tema.

[216] Commissione delle Comunità europee, *The European Community and data processing: Government development aids permitted*, in *Information-Competition*, n. 21, 1972, pp. [disponibile sul sito *Archive of European Integration*, Università di Pittsburgh: link] e Commissione delle Comunità europee, *Community policy on data processing* (Comunicazione della Commissione e del Consiglio). SEC(73) 43 def., Bruxelles, pp. 1 ss. [*ibidem:* link].

non avrebbe facilitato il raggiungimento di una maggior coesione economica e normativa[217].

In ragione di queste osservazioni, dunque, si è avvertita l'esigenza di affrontare la questione in sede europea, tant'è che negli anni successivi la Commissione, il Consiglio e il Parlamento europeo sono intervenuti a più riprese nel promuovere un approccio condiviso su questi temi[218].

---

[217] Commissione delle Comunità europee, *Community policy on data processing*, cit., p. 13 in cui osserva proprio come: «the creation of data banks joined increasingly by international links will oblige the Community to establish common measures for protection of the citizen. When police, and tax, and medical records, and the files of hire purchase companies concerning individuals are held in data banks, the rules of access to this information become vital. This is n matter on which a wide debate is needed in the Community».

[218] Oltre ai già citati interventi, la Commissione, sempre nei primi anni Settanta, dapprima ha promosso l'approfondimento e lo studio di questi temi, commissionando diversi lavori di ricerca poi confluiti nelle premesse di alcune nuove Comunicazioni (Cfr. CCE, *Scientific and technological policy program*, commissionato al Consiglio dalla Commissione il 1° agosto 1973 (COM(73)1250, 25 luglio 29173, *Gazzetta Ufficiale delle Comunità Europee*, Supplemento n. 14/73); CCE, *Communication by the Commission of the European Communities concerning a Community policy for data processing*, in *Information – memo*, P-63/73 [disponibile in *Archive od European Integration*, cit.: link]). In seguito, il Parlamento europeo ha richiamato nuovamente l'attenzione su questi temi con due distinte Raccomandazioni, rispettivamente nel 1975 e del 1976, enfatizzando l'urgenza di un intervento normativo a livello comunitario e suggerendo l'adozione di una direttiva sul rapporto tra libertà individuali e trattamento dei dati (PE, *Resolution of the European Parliament on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing*, 1975, GUCE 60/48; PE, *Resolution of the European Parliament on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing*, 1976, GUCE C100/27). La Commissione, anche sulla base di questi presupposti, negli anni, ha cominciato a promuovere un confronto informale con i rappresentanti di alcuni Stati membri rispetto ai possibili tentativi di armonizzazione della disciplina della materia, anche istituendo un gruppo di lavoro dedicato al rapporto tra elaborazione dei dati e tutela delle libertà (Cfr. CCE, *A four-year programme for the development of informatics in the Community*, commissionato al Consiglio dalla Commissione, 1976 (COM(76) 534 final,)). A queste iniziative era seguita quindi una nuova risoluzione del PE, che su ispirazione del rapporto *Bayerl*, aveva chiarito alcuni punti chiave della futura normativa, sottolineando poi, con alcune raccomandazione, l'importanza di alcuni obblighi e diritti, nonché la presenza delle autorità indipendenti (Cfr. PE, *Resolution of the European Parliament on the protection for the rights of the individual in the face of the technical progress in the field of automatic data processing*, 1979, GUCE C140/34; PE, *Recommendations from Parliament to the Commission and Council pursuant to paragraph 10 of the motion for a resolution concerning the principles which should form the basis of Community norms on the protection of the rights of the individual in the face of developing technical progress in the field of data processing*). Molto ci si era attesi, infine, dalla proclamazione della Convenzione n. 108 del 1981, promossa dal Consiglio d'Europa, cui immediatamente era seguita una raccomandazione da parte della Commissione ad una pronta ratifica del testo da parte degli Stati membri (Cfr. CCE, *Raccomandazione della Commissione del 29 luglio 1981 concernente una convenzione del Consiglio d'Europa sulla protezione delle persone per quanto riguarda*

Delineate così le questioni e il *modus operandi*, erano emersi però alcuni seri problemi nell'addivenire ad una disciplina comune sulla protezione dei dati. Nonostante le istituzioni comunitarie fossero guidate soprattutto da obiettivi di natura economica, forse per la prima volta si intuiva chiaramente come in questo settore la tutela dei diritti avrebbe giocato un ruolo essenziale, soprattutto considerate le forti implicazioni costituzionali della materia in oggetto[219]. In particolare, si erano riscontrati tre ordini di questioni. Innanzitutto, si era ravvisato un primo punto critico nell'individuazione dell'oggetto di tutela, dal momento che le leggi nazionali avevano dato spazio a diversi interessi, tutti riconducibili ai valori della *privacy,* ma certo non limitati alla sola tutela della dimensione privata[220]. Allo stesso modo, risultava problematico stabilire l'ambito di applicazione della

---

*l'elaborazione automatica dei dati a carattere personale (81 /679/CEE),* GUCE L246/31, *considerando* 5.) Ciononostante, anche considerando lo scarso attivismo dimostrato da parte di molti Stati membri, alla fine degli anni Ottanta, ci si era comunque attivati in via definitiva all'adozione di una disciplina unitaria a livello comunitario, inaugurando i lavori con le proposte presentate nel 1990 nell'ambito del c.d. pacchetto *data protection.*

[219] Commissione delle Comunità europee, *Community policy on data processing*, cit., p. 13. Si continua infatti sottolineando come quella dei dati personali sia una materia in cui un dibattito in sede europea sia quanto mai necessario, e dunque sia imprescindibile prendere gli opportuni provvedimenti. «In view of *its basic constitutional importance*, the Commission believes that public "hearings" on the matter are desirable. It would be better for the Community *to seek a genuine political consensus* on this matter now with n view to establishing common ground rules, than to be obliged to harmonise conflicting national legislation later on». (corsivo aggiunto). Il tema è poi stato affrontato con la stessa sensibilità anche da parte di Altiero Spinelli, nel marzo del 1974, in cui nuovamente si sono evidenziate le implicazioni costituzionali legate alla tutela dei diritti e al trattamento dei dati personali, incoraggiando ulteriori approfondimenti in vista di una futura disciplina comunitaria.

[220] Si osserva come sebbene all'inizio le istituzioni europee avessero mantenuto un'impostazione abbastanza aperta, volta a considerare nell'analisi delle diverse questioni una pluralità di diritti legati al trattamento dei dati personali, nel corso delle discussioni si siano registrati degli andamenti altalenanti, spesso spostati a favore di una tutela incentrata sulla *privacy* (Cfr. PE, *Resolution of the European Parliament on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing*, 1975, § 2; PE, *Resolution of the European Parliament on the protection for the rights of the individual in the face of the technical progress in the field of automatic data processing*, 1979, p. 35). Come osservato, tuttavia, in molti casi questo richiamo alla nozione di *privacy* è stata attribuita ai problemi legati al multilinguismo delle istituzioni comunitarie, osservando come comunque tra le diverse versione degli atti spesso si riscontrino traduzioni non perfettamente equivalenti (Cfr. G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection in the EU*, cit., pp. 120-121).

disciplina, soprattutto in merito alla possibilità di prevedere comuni regole di condotta tanto per i soggetti pubblici quanto per quelli privati.

Non ultimo, l'ipotesi di adottare una normativa di carattere generale a livello comunitario aveva sollevato una serie di dubbi circa la necessarietà di un simile intervento, soprattutto alla luce di quanto suggerito dal principio di sussidiarietà[221].

Chiariti i nodi problematici che si frapponevano all'adozione di una normativa europea, non vanno trascurati i problemi emersi – per contro, però – nell'attuazione dei precedenti tentativi di armonizzazione.

Come già ricordato[222], in quegli stessi anni, le medesime questioni erano state affrontate anche in seno al Consiglio d'Europa fino all'approvazione della Convenzione n. 108; un atto che, quanto meno nelle intenzioni, avrebbe dovuto costituire un primo punto di incontro per favorire un approccio più omogeneo alla protezione dei dati personali.

In ambito comunitario quel primo tentativo era stato accolto con un certo entusiasmo, soprattutto da parte della Commissione già propensa al riconoscimento di uno specifico diritto alla protezione dei dati come *addendum* alla Cedu[223]. Tuttavia, guardando all'inerzia e al ritardo con cui molti Stati si erano adoperati rispetto alla ratifica e al recepimento di tale normativa, detta soluzione aveva destato molte

---

[221] Soprattutto negli anni Settanta, ancora agli inizi del dialogo su questi temi, alcuni membri del Parlamento europeo avevano sottoposto all'attenzione dell'Assemblea alcune perplessità circa la necessità di un intervento coordinato da parte di Bruxelles (Cfr. Interrogazione n. 193/73 sulla protezione della privacy dei cittadini comunitari, come citato in G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection in the EU*, cit., pp. 113). In molti, infatti, come più volte ricordato, si stavano intraprendendo delle iniziative autonome, condividendo peraltro alcuni principi e orientamenti comuni. Per contro, però, la Commissione arrivò presto a concludere sull'assoluta necessità di un'iniziativa condivisa a livello europeo; posizione confermata in seguito dai ritardi e le reticenze registrate nella ratifica della Convenzione n. 108 da parte di molti Stati membri.

[222] Cfr. Capitolo 1, § 2.2.

[223] Cfr. CCE, *Raccomandazione della Commissione del 29 luglio 1981 concernente una convenzione del Consiglio d'Europa sulla protezione delle persone per quanto riguarda l'elaborazione automatica dei dati a carattere personale (81 /679/CEE)*, cit., pt. 2.

perplessità[224]. L'indolenza dimostrata dai legislatori nazionali rispetto agli indirizzi proposti da Strasburgo, infatti, era stato letta come un'evidente prova delle difficoltà che si sarebbero incontrate nell'incoraggiare un *framework* normativo unitario attraverso i tradizionali metodi intergovernativi; una ragione in più procedere con un'iniziativa promossa direttamente da Bruxelles.

Al contempo, il Parlamento europeo aveva sottolineato i limiti dell'iniziativa promossa da Strasburgo, trovandola certo apprezzabile come punto di sintesi, ma comunque inadeguata rispetto agli obiettivi che ci si proponeva di raggiungere a livello comunitario[225]. Considerato il contesto in cui era stato formulato l'accordo, infatti, si è guardato con benevolenza alla possibilità di includere un nuovo diritto alla protezione dei dati personali. Cionondimeno, si è ritenuto necessario adottare quanto prima un atto volto a promuovere anche e soprattutto la circolazione transfrontaliera dei dati – e così il mercato – sulla base dell'art. 100A del Trattato CEE[226].

Di lì a poco, peraltro, la firma dell'Accordo di Schengen (1985) e l'Atto unico europeo (1986) avrebbero dato alcuni fondamentali atti d'impulso al processo di integrazione europea, dettando un'agenda di scadenze in cui la normativa comunitaria in materia di protezione dei dati personali avrebbe costituito un tassello essenziale[227].

---

[224] Prima del finire degli anni Ottanta, infatti, soltanto alcuni Stati avevano provveduto alla ratifica della Convenzione dandovi pronta attuazione all'interno del loro ordinamento nazionale (in tutto 7 di 12 ossia Francia, Danimarca, Francia, Germania, Gran Bretagna, Lussemburgo, Spagna). I rimanenti spesso, pur avendo firmato, non avevano provveduto agli adempimenti necessari alla ratifica (come il Belgio, Irlanda, Italia, Paesi Bassi, Portogallo). In queste considerazioni, peraltro, vanno tenute in considerazione anche alcune situazioni particolari, relative a Stati che, pur non essendo membri dell'Unione, comunque intrattenevano rapporti con le Comunità europee e all'Accordo Schengen (come, ad esempio, la Norvegia, l'Islanda e la Svizzera).

[225] Cfr. PE, *Resolution of the European Parliament on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing* [1982] GUCE C87/39, p. 40.

[226] *Ibidem*.

[227] Con la Convenzione di applicazione dell'Accordo Schengen, come già ricordato (capitolo 1, § 3.1), si puntava alla realizzazione di nuove forme di cooperazione rafforzata all'intento dell'Unione europea, soprattutto nella prospettiva di realizzare uno spazio comune per la libera

Nel 1990, dunque, intercettando le esigenze legate alla creazione della spazio comune e del mercato unico europeo, con una nuova comunicazione la Commissione ha presentato un primo "pacchetto" contenente sei diversi progetti legati alla protezione dei dati personali[228], tra cui – in posizione centrale – la proposta per una direttiva di carattere generale sulla protezione degli individui rispetto al trattamento dei loro dati personali.

Alla luce delle evoluzioni degli ultimi anni e, soprattutto delle future prospettive nel processo di integrazione europea, si cominciava così a tutti gli effetti un nuova pagina del diritto comunitario, mettendo a fuoco per la prima volta il tema dei diritti (e dei dati) in una prospettiva più "costituzionale". Ed è in questa cornice che si andranno ad inserire i diversi tasselli che negli anni hanno concorso al delinearsi di una disciplina europea in materia di *data protection*.

---

circolazione delle persone, delle merci, dei servizi e dei capitali. Per rendere possibile questi obiettivi, si è prevista l'istituzione del Sistema d'informazione Schengen (SIS) (cui si è collegato poi, in seguito, anche il Sistema d'informazione visti; c.d. VIS) e la creazione di un autorità di controllo. Presupposto essenziale per partecipare a queste iniziative, evidentemente, era il fatto che i Paesi aderenti fossero dotati di una normativa atta a garantire una soglia di tutela minima per protezione dei dati personali e così, a livello europeo, un *framework* normativo di riferimento.

Allo stesso modo, l'Atto unico europeo, siglato nel 1986 e poi entrato in vigore l'anno successivo, aveva individuato nel 1992 il termine ultimo per la realizzazione del mercato unico europeo; un progetto che, considerato il peso di settori come l'informatica, le telecomunicazioni e i servizi digitali, non poteva davvero più prescindere dall'adozione di una disciplina comunitaria.

[228] Commissione delle Comunità europee, *Comunicazione della Commissione concernente la protezione delle persone per quanto riguarda il trattamento dei dati personali nella Comunità e la sicurezza dei sistemi d'informazione*, 24 settembre 1990, Bruxelles (COM(90) 314 def.– SYN 287 e 288). Oltre alla proposta di quella che sarebbe stata poi (*a*) la dir. CE 95/46 (SYN 277), il documento conteneva anche (*b*) un progetto di risoluzione dei rappresenti dei governi degli Stati membri delle Comunità europee riunite in sede di consiglio; (*c*) una dichiarazione della commissione relativa all'applicazione alle istituzioni e agli organismi delle Comunità europee dei principi della direttiva del Consiglio concernente la protezione delle persona e relativamente al trattamento dei dati personali; (*d*) una proposta di direttiva del Consiglio sulla protezione dei dati personali nell'ambito delle rete digitali pubbliche di telecomunicazione, con particolare riferimento all'ISDN (rete digitale integrata nei servizi) e alle reti digitali per servizi pubblici di radiotelefonia mobile (SYN 278; le basi per la futura dir. CE 66/97); (*e*) una raccomandazione di decisione del Consiglio relativa all'apertura di negoziati in vista dell'adesione delle Comunità europee alla Convenzione del Consiglio d'Europa sulla protezione delle persone nel trattamento automatizzato dei dati di carattere personale, (*f*) una proposta di decisione del Consiglio nel settore della sicurezza dei sistemi d'informazione.

### *2.2. Una panoramica storica sulla disciplina in materia*

Come ci sarà modo di vedere, le questioni accennate poc'anzi continueranno ad essere una costante; dei continui punti di tensione nell'evoluzione della normativa comunitaria. Nei prossimi paragrafi, quindi, si analizzeranno brevemente i contenuti dei principali atti che, a partire dalla seconda metà degli anni Novanta, hanno disciplinato tale materia. L'obiettivo è quello di cogliere le caratteristiche del quadro d'insieme e le evoluzioni nella cultura e nell'approccio ai problemi di cui si è discusso finora.

#### *a. La direttiva n. 95/46*

Com'è facile immaginare, i problemi riscontrati nelle prime iniziative promosse dalla istituzioni europee certo non erano venuti meno. Con gli accordi di Schengen, tuttavia, si è segnato un punto di non ritorno, tanto da rendere urgenti degli opportuni compromessi.

La direttiva del 1995 ha avuto come primo obiettivo quello di promuovere a livello comunitario l'armonizzazione della disciplina sulla protezione dei dati personali dei diversi Stati membri. In linea con tali premesse[229], dunque, la normativa mirava a raggiungere un duplice scopo: garantire, da un lato, elevati livelli di tutela dei diritti e delle libertà fondamentali degli interessati (e, in particolare, il

[229] Era chiaro che la disciplina comunitaria avrebbe avuto una duplice vocazione: da un lato, la libera circolazione dei dati personali e, dall'altro, la tutela delle informazioni e così dei diritti degli interessati. Affermando come cardine della normativa il principio di protezione elevato ed equivalente[229], in nome di considerazioni prettamente economiche, si puntava infatti ad arrivare un sostanziale livellamento delle garanzie a favore di essenziali diritti della personalità; un obiettivo che, fino ad allora, era risultato irraggiungibile a qualsiasi altra iniziativa.

diritto alla vita privata[230]) e promuovere, dall'altro, la libera circolazione dei dati a livello transfrontaliero[231].

La direttiva europea ha così trovato applicazione rispetto a tutti i trattamenti di dati personali automatizzati e non[232], eccezion fatta per tre categorie di operazioni: quelle non disciplinate dal diritto comunitario; quelle effettuate da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico[233] e quelle in cui il titolare del trattamento non sia stabilito nel territorio di uno Stato membro[234]. E ciò a riprova di come, nonostante le perplessità iniziali, la dir. 95/46 sia stata pensata per includere tanto le attività del settore privato, quanto quelle del pubblico[235] (seppur con le debite cautele).

---

[230] Quanto al primo di questi aspetti (*a*), fin da principio la proposta originale e le sue successive modifiche, fino al definitivo, risultano ambigue. Non solo, infatti, spesso l'oggetto di protezione risulta indeterminato ma le stesse allusioni alla protezione dei dati, in quanto tali, emerge come obiettivo incidentale, spesso manifestando anche evidenti differenze tra le diverse traduzioni. Va rilevato come, inizialmente, si fosse puntata l'attenzione soprattutto sulla tutela della *privacy* e come, a differenza delle altre versione, nella stesura inglese non vi fosse comunque nessun accenno alla natura della protezione dei dati personali come diritto fondamentale. Nel corso del tempo, poi, in particolare a seguito delle modifiche suggerite dal Parlamento e confluite nella versione del 1992, l'impostazione è gradualmente cambiata, transitando verso la formulazione odierna, per cui l'obiettivo della disciplina consiste nella «tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali» (art. 1, § 1).

[231] Art. 1.

[232] Art. 3, § 1 (letteralmente: « si applicano al trattamento di dati personali interamente o parzialmente automatizzato nonché al trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi»). Il primo elemento innovativo, innanzitutto, riguarda i tipi di trattamento inclusi, poiché, a differenza della Convenzione n. 108, in questo caso sono stati contemplati non solo i trattamenti automatizzati ma anche l'archivistica cartacea, seppur con le debite accortezze

[233] Art. 3, § 2.

[234] Art. 4.

[235] Una scelta giustificata anche e soprattutto dall'approccio sviluppato in seno alla Convenzione n. 108, su influsso delle esperienze dell'ordinamento francese e tedesco. Cfr. H. HEIL, *Directive 95/46/EC of the European Parliament and of the Council: Introductory Remarks,* in A. BÜLLESBACH et al. (a cura di), *Concise European IT Law*, Alphen aan den Rijn, Kluwer International Law, 2010, come citato in G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection in the EU*, cit., p. 126; O. LYNSKEY, *The Foundation of EU Data Protection Law*, Oxford, Oxford University Press, 2015, p. 16.

Se si scorre rapidamente il testo normativo si coglie immediatamente come l'impronta rigida che aveva caratterizzato la prima proposta, nel tempo abbia trovato molti accomodamenti, escludendo non solo le materie estranee alle competenze comunitarie, ma anche tutta una serie di casi legati a questioni di interesse nazionale. L'elenco ha incluso «la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico, laddove tali trattamenti siano connessi a questioni di sicurezza) nonché varie attività in materia di diritto penale»[236], cui si sono aggiunte poi una serie di *addenda* in campo amministrativo e giuslavoristico (tutt'altro che secondarie)[237].

Per evitare ulteriori ritardi nell'*iter* legislativo, infatti, dopo il Trattato di Maastricht[238], il legislatore europeo aveva sagomato una disciplina che, seppur trasversale, potesse essere ricondotta pienamente entro il perimetro delle competenze afferenti al c.d. primo pilastro, lasciando al legislatore nazionale (e alla sua discrezionalità) il compito di disciplinare gli altri settori[239].

Quanto ai contenuti, la direttiva innanzitutto ha codificato i principi fondamentali della disciplina; capisaldi rimasti pressoché invariati fino ad oggi. Si legge infatti che le informazioni personali devono essere trattate lealmente e

---

[236] Art. 3, § 2, pt. 1.

[237] Soprattutto si considera il margine di discrezionalità dello legislatore in queste materie, gli obblighi di collaborazione che possono essere imposti *ex lege* agli operatori privati in qualche modo coinvolti e, in questo modo, la pervasività e l'intrusività delle misure in questione.

[238] La scelta originaria e così i suoi sviluppi successivi si spiegano anche e soprattutto alla luce della complessiva evoluzione del processo di integrazione comunitaria. Il Trattato di Maastricht, intervenuto nelle more dell'*iter* di approvazione della direttiva, aveva assimilato l'*acquis* di Schengen, suddividendo le competenze fondamentale dell'Unione in tre macro-aree, anche dette "pilastri": al primo sono state ricondotte le politiche per il funzionamento del mercato interno; al secondo, la politica estera e la sicurezza comune; al terzo, la cooperazione nei settori della giustizia e degli affari esteri. Sebbene il quadro istituzionale fosse caratterizzato da un impronta complessivamente unitaria, considerando i tre pilastri tra loro funzionalmente connessi, le modalità di azione, in ciascuno di essi, erano radicalmente diversi. A differenza delle materie relative alla cooperazione europea, per il secondo e il terzo pilastro le procedure decisionali erano molto meno agevoli; ragione che ha indotto il legislatore europeo a mantenersi il più possibile entro il perimetro del primo, onde non rallentare ulteriormente l'*iter* di approvazione della direttiva.

[239] L. DANIELE, *Diritto dell'Unione europea*, Milano, Giuffrè, 2018, pp. 24 ss.; R. ADAM, A. TIZZANO, *Manuale di diritto dell'Unione europea,* Torino, Giappichelli, 2017, pp. 20 ss.

lecitamente, per finalità determinate, esplicite e legittime[240]; quanto alla qualità dei dati, questi devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono raccolti e utilizzati[241]. Il titolare del trattamento, infine, si impegna a conservare i contenuti in forma identificativa per il solo tempo necessario[242], adottando tutte le misure necessarie affinché le informazioni siano esatte (e, se necessario, aggiornate) provvedendo alla cancellazione e alla rettifica dei contenuti inesatti o incompleti[243].

Ciò premesso, il titolare sarebbe stato legittimato a trattare i dati personali soltanto nei casi previsti dalla legge, stabilendo un'implicita riserva. Secondo quanto previsto, la normativa, all'epoca, ha individuato dunque una serie di ipotesi, come il caso in cui l'interessato abbia prestato il proprio consenso; quando l'utilizzo dei dati sia necessario per l'esecuzione di un contratto già concluso; quando sia indispensabile per adempiere un obbligo legale; quando sia indispensabile per salvaguardare un interesse vitale per il soggetto interessato; laddove sia necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri e – non ultimo – quando risulti necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento (a condizione però che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata)[244].

Dopo aver previsto alcune particolari cautele per il trattamento dei dati sensibili[245] e la tutela della libertà di informazione[246], la dir. 95/46 ha individuato una

---

240 Art. 6, § 1, lett. *a*) e *b*).
241 *Ibidem*, lett. *c*).
242 *Ibidem*, lett. *e*).
243 *Ibidem*, lett. *d*).
244 Art. 7.
245 Art. 8.
246 Art. 9.

serie di prerogative in capo all'interessato; strumenti necessari per far valere il suo diritto all'autodeterminazione informativa[247].

È rimasto un presupposto essenziale che il titolare proceda alle diverse operazioni con la massima trasparenza, fornendo all'interessato tutte le informazioni necessarie a conoscere e comprendere le caratteristiche della sua attività e le logiche del trattamento[248]. La *summa* poi continua includendo il diritto dell'interessato ad accedere ai dati personali che lo riguardano[249], il diritto di opporsi al trattamento in qualsiasi momento per motivi legittimi legati alla sua situazione particolare[250] e il diritto di non essere sottoposto a processi di decisione individuale automatizzata[251] (un'eventualità quest'ultima guardata con particolare sospetto visto il rischio di estraniare la persona dalle logiche inerenti le decisioni che la interessato)[252].

---

[247] è senz'altro uno degli ambiti in cui emergono con maggior forza le tensioni che si contrappongono in questa disciplina. Una volta sanciti i diritti dell'interessato, il legislatore europeo, per contemperare le contrapposte aspettative che si incontrano a livello nazionale subito aggiunge come corollario una serie di deroghe e restrizioni (artt. 14, art. 15, § 2) che, di fatto, possono minimizzare l'effettiva portata della garanzia o, quanto meno, l'obiettivo di garantire a livello comunitario un livello di tutela elevato e condiviso da tutti gli Stati membri.

[248] Artt. 10 e 11.

[249] Art. 12.

[250] Art. 14.

[251] Art. 15.

[252] Quanto invece ai profili più legati al rapporto tra diritto e tecnologia, già nel corso dei lavori erano emerse preoccupazioni e dubbi per i futuri sviluppi della società dell'informazione. Come documentano i lavori preparatori alla direttiva in esame, oltre ai diritti di cancellazione, rettifica e "congelamento" dei dati raccolti – desumibili anche dai principi generali – viene prestata particolare attenzione alle questioni inerenti i processi decisionali automatizzati. In soli due anni, dal 1990 al 1992, la formulazione del futuro articolo 15 subisce infatti importanti modifiche. Analizzando al *ratio* di questa disposizione, infatti, si osserva come adottando questo tipo di sistemi il rischio sia quello di ridurre la persona soltanto alla sua proiezione informativa (alla sua "*data shadow*") e così di escluderlo, di fatto dai processi decisionali che lo interessano; una consapevolezza ancor maggior nel momento in cui si osserva: «the danger of the misuse of data processing in decision-making may become a major problem in future: the result produced by machine, using more and more sophisticated software, and even expert systems, had an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities».

Il titolare del trattamento, in tutto ciò, assieme ai suoi collaboratori, conserva l'obbligo di garantire la riservatezza dei dati trattati[253] e la sicurezza dei sistemi di cui si avvale[254]. Questi soggetti, in particolare, sono tenuti a collaborare con le autorità garanti soprattutto per quanto riguarda i processi in cui i dati vengono trattati in modo totalmente o parzialmente automatizzato[255]. Inoltre, prima di cominciare operazioni particolarmente rischiose per i diritti dell'interessato, era previsto che gli stessi ottenessero le debite autorizzazione, come forma di controllo preventivo[256].

Infine, vi erano le disposizioni inerenti i ricorsi giurisdizionali, alle sanzioni e ai profili di responsabilità[257], nonché la disciplina relativa al trasferimento dei dati verso Paesi terzi[258]. A chiudere il cerchio, si trova la definitiva istituzionalizzazione delle Autorità di controllo a livello nazionale, con una serie di norme volte a sancirne i compiti e le prerogative di autonomia e indipendenza[259].

Tornando alle riflessioni accennate nel paragrafo precedente, si possono fare alcuni primi rilievi. L'effettività delle garanzie apprestate dalla direttiva 95/46, infatti, sarebbe dipesa, da un lato, dall'implementazione della disciplina a livello nazionale e, dall'altro, dalla puntualità della normativa rispetto agli sviluppi delle tecnologie informatiche e digitali[260].

Quanto al primo di tali punti, è interessante notare come, già nelle sue prime pronunce su questa direttiva, i giudici lussemburghesi abbiano abbracciato un

---

253 Art. 16.
254 Art. 17.
255 Artt. 18-19.
256 Art. 20-21.
257 Artt. 22-23-24.
258 Artt. 25-26.
259 Artt. 28-29-30.
260 In questo lavoro mancheranno il tempo e lo spazio per affrontare compiutamente l'*iter* di approvazione e le evoluzioni che hanno interessato la dir. 66/97 CE. Si affronterà invece, seppur brevemente, la successiva normativa introdotta dalla dir. 58/2002 UE, riprendendo in quella sede, per cenni, anche i precedenti tentativi di regolamentazione. Per ogni approfondimento, tuttavia, si rimanda a G. BUTTARELLI, *Banche dati e tutela della riservatezza*, cit., pp. 59 ss.; P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione europea*, cit., cap. 4; G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection in the EU*, cit., pp. 140 ss.

approccio particolarmente garantista. La Corte, infatti, da subito si è orientata verso un'interpretazione ampia delle definizioni di base, ampliando così l'ambito di applicazione a fattispecie assai diverse tra loro[261]. Contrariamente alle aspettative, dunque, è prevalso fin da principio un'interpretazione *right oriented*[262], seppur ancorata ai valori della *privacy* quale principio del diritto comunitario[263].

Quanto al secondo punto, rispetto alle evoluzioni della tecnologia informatica in quegli stessi anni erano stati avanzati anche altri progetti, complementari alla dir. 95/46, e volti a promuovere una più puntuale disciplina dei servizi della c.d. società dell'informazione. Con la conversione al digitale – si era osservato – il settore delle comunicazione, così come molti altri, transitava dai sistemi analogici verso «l'introduzione di centrali completamente computerizzate» in cui «l'elaborazione e la trasmissione di ogni tipo d'informazione trasmessa con reti di telecomunicazione – voce, dati e immagini – [sarebbe avvenuta *n.d.a.*] mediate un sistema numerico binario»[264]. Si intuiva dunque in modo sempre più chiaro come la protezione dei dati personali, con l'andar del tempo, avrebbe finito con l'intercettare temi e materie prima di allora ricondotte ad altri ambiti, facendo di questa normativa una disciplina di portata sempre più trasversale[265]. E questo non solo per la promozione del mercato interno, ma anche e soprattutto da un punto di vista istituzionale, a livello europeo così come a livello nazionale.

---

[261] CGUE, sent. 14 settembre 2000, *Fisher* (causa C-369/98), §§ [23-25]

[262] CGUE, sent. 20 maggio 2003, *Österreichischer Rundfunk e a.* (cause C-465/00, C-138/01), §§ 68, 41-42; CGUE, sent. 6 novembre 2003, *Lindqvist* (causa C-101/01), § 99.

[263] CGUE, *Fisher*, § 34, in cui la Corte osserva come tanto alcuni *considerando* della direttiva 95/46 (nn. 10 e 11) quando la Convenzione n. 108 e i riferimenti Cedu (art. 8) suggeriscono una simile soluzione. Tesi sostenuta in G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection in the EU*, cit., p. 132, spec. nota n. 149.

[264] COM (90) 314 def. SYN 287 e 288, pp. 89 ss., con riferimento al concetto di "digitalizzazione".

[265] Una serie di preoccupazioni che cominciano ad essere registrate soprattutto a partire dal maggio 1994, con il c.d. rapporto Bangermann, *Europe and the global information society*.

*b. Il regolamento 2001/45*

Di lì a pochi anni, a cambiare il modo in cui la protezione dei dati personali era stata intesa fino a quel momento, sarebbe intervenuto il reg. 2001/45. Sebbene infatti le istituzioni europee si fossero già impegnate a conformarsi alla disciplina della dir. 95/46, è solo con il Trattato di Amsterdam che ci si orienta verso una prima costituzionalizzazione di questa materia a livello europeo.

Il nuovo art. 286 TCE aveva stabilito che la normativa comunitaria sulla protezione dei dati personali di lì in avanti dovesse trovare applicazione anche agli organismi europei, prevedendo inoltre la presenza di un'autorità indipendente preposta a vigilare sulla corretta applicazione della disciplina da parte delle istituzioni comunitarie[266].

Quelle che fino a quel momento erano state lette soltanto come delle regole atte a promuovere lo sviluppo del mercato comune, si apprestavano così a diventare a tutti gli effetti una materia di diritto costituzionale europeo, ponendo i fondamenti per una più chiara definizione dei rapporti verticali tra i cittadini e l'Unione[267].

Quanto ai contenuti, non si può fare a meno di notare come il reg. 2001/45 seguisse per certi versi una logica in parte differente da quella fatta propria dalla direttiva "madre". L'impianto della disciplina, infatti, pur dedicando particolare attenzione ai profili legati alla libera circolazione dei dati, si è caratterizzato per un

---

[266] Art. 286 TCE

[267] Come inizialmente suggerito a più riprese dal Parlamento e dalla Commissione la protezione dei dati personali entrava così implicitamente nel novero dei diritti fondamentali tutelati a livello comunitario, proprio secondo l'impostazione tradizionalmente sostenuta dalla Cedu e dalla Convenzione di Strasburgo. Cfr. P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione europea*, cit., p. 83.

forte approccio *right oriented*, facendo di questo secondo aspetto il *focus* della normativa [268].

Questo leggero cambio di prospettiva documenta il chiaro intento di promuovere un regime di effettiva trasparenza in gran parte dei trattamenti operati a livello comunitario, garantendo così all'interessato un maggior controllo sull'utilizzo dei propri dati.

Tale nuova sensibilità si rende particolarmente evidente nella ridefinizione degli oneri in capo al titolare del trattamento. Sebbene l'impostazione generale, infatti, rispecchiasse la struttura della direttiva "madre", è stato introdotto innanzitutto un *dovere* generale di informazione a favore dell'interessato[269], rendendo obbligatorio fornire un quadro completo delle condizioni di utilizzo dei dati e allegando poi – ove necessario – il fondamento giuridico del trattamento, l'origine dei contenuti raccolti presso terzi[270], i limiti di tempo della conservazione e il diritto di rivolgersi in ogni momento al Garante europeo.

In quest'ottica, si è registrato anche un contestuale rafforzamento dei diritti previsti a tutela dell'interessato. Il catalogo previsto dal regolamento, sostanzialmente, ha consentito di far valere pretese analoghe a quelle che avevano già trovato spazio nella dir. 95/46. Tuttavia, considerati gli strumenti ivi previsti, la disciplina qui ha potenziato ulteriormente le facoltà di controllo sul trattamento dei propri dati personali. È stato previsto, ad esempio, che la persona possa opporsi al

---

[268] Nella prima versione dell'art. 1, infatti, quanto all'obiettivo del regolamento, il testo si limitava a disporre: «le istituzioni e gli organismi istituiti dai trattati che istituiscono le Comunità europee o sulla base di tali trattati (in prosieguo: «le istituzioni e gli organismi comunitari») garantiscono, conformemente alle disposizioni del presente regolamento, *la tutela dei diritti e delle libertà fondamentali delle persone fisiche*, ed in particolare il diritto alla riservatezza per quanto attiene al trattamento dei dati personali» (Cfr. COM (1999) 337 def., art. 1, corsivo aggiunto). È solo nella versione definitiva che vengono introdotti gli attuali riferimenti alla libera circolazione delle informazioni, intesa sia da una punto di vista interno (rispetto ai rapporti organici) sia verso l'esterno, nelle relazioni con le parti terze.

[269] Art. 11. A differenza di quanto previsto dalla dir. 95/46, infatti, la norma in esame prevede che vengano fornite all'interessato *tutte* le informazioni, rendendo così obbligatorie anche quelle che la direttiva aveva previsto come facoltative.

[270] Art. 12.

trattamento per «motivi preminenti e legittimi connessi alla sua situazione particolare»[271] o che possa aver accesso ai contenuti che la riguardano liberamente e in ogni momento, in modo gratuito e in tempi prestabiliti[272]. Per quanto poi riguarda le decisioni individuali automatiche, la disciplina ha riconosciuto nuove garanzie e prerogative, disponendo che, quando vengano adottati questi sistemi, siano comunque previste adeguate misure di tutela, «facendo in modo che questi possa esprimere il proprio parere»[273]. Infine, nell'ipotesi in cui, per qualsiasi motivo, si rendesse necessario limitare i diritti dell'interessato o derogare le ordinarie misure di protezione, il reg. 45/2001 ha previsto che la persona sia informata dei motivi di tali limitazioni e, qualora sia inibito l'accesso ai dati, che questa abbia diritto ad essere assista dal Garante europeo per ottenere dei controlli *ex post* sulle attività di trattamento che la riguardano[274].

Quanto ai contenuti di natura più tecnica, considerate le finalità per cui è stata introdotta, la disciplina ha introdotto in una serie di previsioni relative ai presupposti e alle condizioni di utilizzo dei dati personali da parte delle istituzioni comunitarie, adattando i principi della direttiva «madre» a questo diverso contesto. In particolare, hanno trovato spazio in quest'atto sia le norme relative al trasferimento di informazioni interno agli organismi europei[275], sia quelle inerenti al trasferimento di dati verso enti e attori soggetti alla disciplina ordinaria[276].

In una complessa trama di disposizioni, in cui spesso si è ammesso il cambiamento di finalità in corso d'opera[277], si sono aggiunte, quindi, una serie di ulteriori accorgimenti che, nel tempo, hanno contribuito a consolidare l'architettura della protezione dei dati nel contesto europeo.

---

271 Art. 18, lett. *a*).
272 Art. 13.
273 Art. 19.
274 Art. 20, §§ 3 e 4.
275 Art. 7.
276 Art. 8.
277 Art. 4.

Per garantire maggior trasparenza circa le logiche di trattamento, è stata introdotta, ad esempio, la figura del responsabile della protezione dei dati personali[278]; un soggetto indipendente presente presso ogni istituzione, dotato di specifiche competenze in materia di *data protection*. Questi, da un lato, è preposto a vigilare sul corretto adempimento degli obblighi previsti dalla disciplina e, dall'altro, ha il compito di interfacciarsi con i cittadini, così da garantire che le pretese di questi ultimi vengano prontamente ascoltate[279]. Nell'ottica di promuovere la trasparenza e la sicurezza delle diverse attività, il primo compito di questo funzionario è quindi quello di tenere un registro di tutti i trattamenti svolti[280], facendo in modo che siano adottate adeguate misure organizzative per proteggere la riservatezza e l'integrità dei dati, sia rispetto agli utilizzi interni sia alle minacce esterne[281].

In linea con quanto previsto dall'art. 286 TCE, infine, è stata prevista l'istituzione una figura cui già si è avuto modo di accennare, ossia il Garante europeo per la protezione dei dati personali (GEPD o *EDPS*). Analogamente a quanto previsto dalla dir. 95/46, a quest'autorità indipendente viene riconosciuto innanzitutto un potere di controllo preventivo sui trattamenti che, per loro natura, possono rappresentare rischi specifici per i diritti e le libertà dell'interessato[282]. A ciò si è aggiunto l'obbligo per le istituzioni europee di informare il GEPD nel momento di elaborare e di adottare atti normativi inerenti la protezione dei dati personali, unitamente ad una serie di altri adempimenti legati al principio di leale collaborazione.

Tutto considerato, dunque, il quadro che si è venuto a delineare rispetto a quanto originariamente previsto dalla dir. 95/46, documenta dei piccoli progressi, graduali ma decisi, che certo non hanno stravolto la fisionomia della disciplina ma

---

278 Artt. 24-25.
279 Art. 24.
280 Art. 26
281 Art. 22.
282 Art. 27.

hanno contribuito ad affrancarla da un'impostazione prevalentemente orientata alla tutela del mercato.

Come osservato nei paragrafi precedenti, non si tratta di un approccio completamente nuovo. La Commissione, infatti, sin da principio aveva guardato alla protezione dei dati personali come a un tema di forte impatto costituzionale, incoraggiando, in tal senso, il riconoscimento di un diritto fondamentale *ad hoc* proprio in materia di autodeterminazione informativa[283].

Rispetto alla novella introdotta dal Trattato di Amsterdam, tuttavia, leggendo l'art. 286 TCE, l'auspicio sembrava quello di veder definitivamente ampliato l'ambito di applicazione della disciplina a *tutte* le attività di trattamento operate dalle istituzioni europee, favorendo un approccio più affine alla tutela dei diritti. La riforma dei Trattati istitutivi, infatti, in prospettiva, lasciava intuire come il processo di integrazione europea avrebbe portato ad un progressivo consolidamento delle competenze comunitarie in diversi settori, aggiungendo nuovi tasselli per la definizione di una vera e propria pubblica amministrazione comunitaria[284].

È in quest'ottica, dunque, che possono essere lette le conclusioni del Consiglio europeo di Colonia del 1999, circa la proposta di elaborare una Carta dei diritti fondamentali dell'Unione europea[285]. Tuttavia, quanto alla possibilità di ipotizzare una competenza generale dell'Unione europea sulla protezione dei dati personali, i

283

284 Una consapevolezza ormai matura, come si legge anche nel in merito alla «Proposta di regolamento del Parlamento europeo e del Consiglio 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» (2000/C 51/13) in cui si legge proprio come le condizioni che giustificano l'adozione del regolamento risiedano nel fatto che: «il trattamento dei dati personali è un'operazione praticata correntemente dalle istituzioni e dagli organi comunitari, in special modo dalla Commissione, nell'ambito della loro attività. La Commissione procede allo scambio di dati personali con gli Stati membri nel quadro della politica agricola comune, per la gestione del regime doganale, dei fondi strutturali e di altre politiche comunitarie».

285

tempi non erano ancora maturi[286]. Visto il complesso sistema di deroghe già previsto dal diritto comunitario una simile soluzione, in quel momento, avrebbe potuto essere percepita come una sorta di forzatura, contradditoria rispetto ai principi stessi dell'ordinamento.

### *c. La direttiva 2002/58*

Quanto agli sviluppi tecnologici, a corollario della disciplina introdotta dalla dir. 95/46, era stata prontamente adottata da lì a due anni la direttiva 97/66.

Come ricordato, infatti, contestualmente alla proposta di una direttiva sulla protezione dei dati personali, era stato presentato anche un progetto per regolamentare l'utilizzo di queste informazioni nel campo delle telecomunicazioni.

Senz'altro il primo merito della direttiva 97/66 era stato quello di aver cominciato a sviluppare in modo analitico le questioni giuridiche legate allo sviluppo di nuovi sistemi di comunicazione. Tuttavia, come si evince dall'architettura complessiva della disciplina[287], il legislatore aveva ragionato soprattutto in una logica

---

[286] La Commissione nella prima versione della proposta di regolamento aveva introdotto la possibilità di istituire una disciplina con un campo di applicazione particolarmente ampio, prevedendo che la normativa potesse applicarsi «al trattamento di dati personali da parte di *tutte le istituzioni* e *tutti dli organismi comunitari*» (COM (1999) 337 def., art. 3, § 1, corsivo aggiunto) senza distinzioni rispetto al fatto che siano disciplinati nell'ambito dei Trattati CE, CECA, EURATOM, ovvero al Titolo V del Trattato sull'Unione (come, ad esempio, la pubblica sicurezza, la difesa, la sicurezza dello Stato e le attività in materia penale). Tuttavia, nonostante quest'impostazione avesse trovato sostegno [Parere del Comitato economico e sociale (2000/C 51/13), spec. § 1.7, circa le critiche all'eventuale esclusione di Europol, così come per gli altri organi del terzo pilastro], il Parlamento e il Consiglio, alla lettura della proposta iniziale, hanno preferito adottare un approccio più moderato, limitando la portata dell'art. 3 ai trattamenti che avvengono «nell'esercizio di attività che rientrano in tutto o in parte nel campo di applicazione del diritto comunitario» (A5-0279/2000, emendamento n. 11, p. 14).

[287] Sebbene nelle definizioni iniziali i concetti di «rete pubblica di telecomunicazione» e di «servizio di telecomunicazione» (art. 2, lett. *c* e *d*) si prestino a coprire un perimetro relativamente ampio [la prima, infatti, individua genericamente «i sistemi di trasmissione e, se del caso, le attrezzature di commutazione e altre risorse che permettano la trasmissione di segnali tra determinati punti terminali tramite fili, radio, mezzi ottici o altri mezzi elettromagnetici, utilizzati in

di breve periodo concentrandosi sulle reti di telefonia fissa e telefax e lasciando in secondo piano invece i servizi legati alle comunicazioni digitali e all'uso di Internet[288].

La Commissione, dunque, aveva promosso un secondo pacchetto di misure relative alle reti e ai servizi di comunicazione elettronica[289], avanzando la proposta di abrogare la prima direttiva per far spazio ad una nuova normativa al passo con il progresso delle tecnologie digitali[290].

---

tutto, o in parte, per la fornitura di servizi di telecomunicazione offerti al pubblico»; la seconda, «servizi la cui fornitura consiste in tutto o in parte nella trasmissione e nell'inoltro di segnali su reti di telecomunicazione, ad eccezione della radiodiffusione e della telediffusione»] se si prendono in analisi le disposizioni di dettaglio si coglie come il legislatore si concentri soprattutto sulle reti di telefonia, prevedendo una particolare disciplina, ad esempio, sulla presentazione e restrizione dell'identificazione della linea chiamante (art. 8), sugli elenchi degli abbonati (art. 11) o sulle chiamate indesiderate (art. 12).

[288] Soprattutto verso la fine degli anni Novanta si è registrata una rapida diffusione dei servizi di comunicazione vocale tramite internet (i c.d. servizi *VoIP*; *voice over IP*); una tecnologia che non solo ha preteso congrui adeguamenti della disciplina sulla protezione dei dati personali con riferimento alla libertà di comunicazione, ma che ha anche rivoluzionato i precedenti modelli di mercato in questo settore, come vi sarà modo di analizzare in seguito (§ ). Negli anni, il Gruppo Articolo 29 – il comitato di lavoro previsto dalla dir. 95/46 per promuovere un approccio comunitario integrato sulla protezione dei dati personali, aveva svolto sul punto diversi studi. Tali riflessioni erano infine confluite nel documento di lavoro *Tutela della vita privata su Internet – Un approccio integrato dell'EU alla protezione dei dati* on-line (WP37) del 21 novembre 2000. Con quell'atto, per la prima volta, si era proposta un'analisi sistematica sui servizi disponibili in Internet, sulla posta elettronica e sui sistemi di navigazione e ricerca, fornendo le coordinate per l'aggiornamento della disciplina in diversi settori.

[289] Si rimanda alle proposte della Commissione per: (*a*) una direttiva relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime (COM(2000) 384 def.); (*b*) una direttiva relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (COM(2000) 385 def.); (*c*) una direttiva relativa all'autorizzazione per le reti e i servizi di comunicazione elettronica (COM (2000) 386 def.); (*d*) una direttiva relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica (COM(2000) 392 def.); (*e*) una direttiva che instituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica (COM(2000) 393 def.).

[290] Commissione europea, *Proposta di direttiva del Parlamento e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (presentata dalla Commissione)* (COM(2000) 385 def.). Come si osserva nella relazione, la nuova direttiva ha lo scopo di sostituire la precedente – la dir. CE 97/66 – senza introdurre variazioni di grande rilievo nelle disposizioni sostanziali ma adeguandone e aggiornandone i contenuti ai nuovi sviluppi dei servizi e delle reti di comunicazione elettronica (§§ 1 e 3).

Tale iniziativa si è tradotta nell'adozione della dir. 2002/58, «relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche»; una disciplina il cui obiettivo principale è quello di venire incontro, per l'appunto, alle nuove esigenze legate alla *digital privacy*.

Sul piano sostanziale, l'architettura normativa consiste in una serie di misure volte a tutelare i diritti e le libertà fondamentali con riferimento ai trattamento delle informazioni personali nel settore delle comunicazioni elettroniche, ponendo l'accento, in particolare, sul rispetto della vita privata[291]. Precisando quanto previsto dalla dir. 95/46, si conferma quindi uno schema bipartito in cui la tutela della persona è intesa come precondizione necessaria allo sviluppo del mercato, e così alla libera circolazione dei dati e delle nuove tecnologie all'interno dello spazio economico europeo.

Data la necessità di sostituire la precedente normativa per adattare il quadro di tutele alle caratteristiche dei nuovi sistemi sviluppati sull'onda della convergenza digitale, la disciplina così introdotta si caratterizza per la presenza di alcuni accorgimenti di natura tecnico-procedurale.

La riforma, innanzitutto, si ispira al principio di «neutralità tecnica», garantendo un livello di tutela uniforme a prescindere dalla tecnologia con cui i servizi possono essere erogati. La precedente disciplina, infatti, aveva fallito nel circoscrivere la portata delle norme a concetti e fattispecie presto superate dall'innovazione[292]. Così, onde evitare di incorrere nello stesso errore, la nuova

---

[291] Art. 1. Considerata però la natura degli interessi coinvolti, a differenza della direttiva "madre", la nuova normativa prevedere un ambito di applicazione più ampio, includendo non solo le persone fisiche ma anche le persone giuridiche, qui tutelate nella loro veste di "abbonati" (art. 1, § 2).

[292] Come si legge, per inciso, al considerando n. 4, si avvertiva infatti la necessità di adeguare la precedente disciplina «agli sviluppi verificatisi nei mercati e nelle tecnologie dei servizi di comunicazione elettronica, in guisa da fornire un pari livello di tutela dei dati personali e della vita privata agli utenti dei servizi di comunicazione elettronica accessibili al pubblico, indipendentemente dalle tecnologie utilizzate».

normativa si caratterizza per la presenza di definizioni plastiche[293], pensate in vista dei futuri sviluppi tecnologici.

In tal senso, meritano particolare attenzione alcune specificazioni relative ai c.d. dati comunicativi, soprattutto per quanto riguarda i dati di traffico e di ubicazione.

I primi certo non costituiscono un'assoluta novità; già in precedenza infatti erano state perviste alcune restrizioni, limitando l'utilizzo di tali elementi alle sole attività di fatturazione. Tuttavia, con l'andare del tempo, si è realizzato l'ulteriore potenziale di questi contenuti, considerati non più delle semplici informazioni "tecniche" bensì elementi in grado di immortalare relazioni, abitudini e condizioni personali (basti pensare a cosa possono svelare le tracce delle varie ricerche *online*)[294].

Nuova risulta invece la categoria dei dati relativi all'ubicazione[295], un sottoprodotto informativo generato automaticamente dalla connessione delle reti cellulari e satellitari. Evidentemente, anche in questo caso il problema era legato alla tracciabilità degli utenti. Il trattamento di questi contenuti, infatti, permette di conoscere e seguire l'esatta localizzazione dei dispositivi; una circostanza che avrebbe potuto ingenerare timori circa il pieno godimento della libertà di circolazione, tanto da rischiare di dissuadere i consumatori dall'utilizzo degli strumenti di navigazione[296].

---

[293] Art. 2. specificando il significato di "chiamata" e "comunicazione" alla luce degli sviluppi delle reti elettroniche, introducendo nuove nozioni atte ad identificare i servizi "a valore aggiunto" e di "posta elettronica" e, soprattutto, rimodulando i concetti relativi ai dati di traffico e di ubicazione.

[294] Relazione introduttiva (COM(2000) 385), § 1.

[295] Art. 2, § 2, lett. *c*) e *considerando* 35.

[296] P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione europea*, cit., p. 202. Considerazioni peraltro già rappresentate ampliamente dalla Commissione, nell'ambito della sua prima proposta in cui, nella relazione si osserva come «occorre guardare con favore ai servizi basati sulla localizzazione dell'utente mobile, in quanto si dimostrano di grande utilità pubblica; [e] d'altra parte, è necessario che siano garantire un'adeguata protezione dei dati e garanzie per la vita privata». «La capacità di trattare dati estremamente precisi in ordine all'ubicazione dell'utente nelle reti di comunicazione mobili – infatti – non deve portare ad una situazione in cui l'utente resti sotto

Alla luce di queste considerazioni, dunque, la dir. 2002/58 promuove un approccio orientato alla *non tracciabilità* degli utenti, ammettendo che i dati comunicativi possano essere utilizzati solo con il consenso dell'interessato, per le attività necessarie all'erogazione del servizio o per la fornitura di prestazioni aggiuntive [297]. Sono ammesse deroghe solamente nei casi in cui l'immediata disponibilità di tali informazioni sia giustificata da una situazione di emergenza, come, ad esempio, la chiamata ricevuta dalle forze di polizia o dai servizi di ambulanza[298].

La normativa poi continua con diverse previsioni relative ai criteri di fatturazione, ai limiti e alle condizioni per l'identificazione e il trasferimento delle chiamate o ai meccanismi di *opt-in* e *opt-out* rispetto agli elenchi degli abbonati[299].

Quel che preme mettere in luce, però, è come, in generale, la dir. 2002/58 abbia contribuito a consolidare alcune tendenze in materia di protezione dei dati personali, mettendo in luce il forte rapporto che lega questa disciplina allo sviluppo tecnologico. Con l'obiettivo di garantire la riservatezza delle comunicazioni e per evitare che i dati e i contenuti trasmessi possano essere intercettati[300], il legislatore infatti impone un generale obbligo di sicurezza rispetto alle tecnologie utilizzate[301], incoraggiando l'utilizzo di particolari accorgimenti tecnici e organizzativi, come, ad esempio, il ricorso alla crittografia o lo sviluppo di nuovi sistemi di *privacy enhancing technology*[302].

---

sorveglianza permanente al punto da trovarsi costretto a non utilizzare affatto i servizi di comunicazione mobile pur di tutela la propria vita privata» (§ 3).

[297] Artt. 8-9 e *considerando* 22.

[298] Art. 10.

[299] Per una panoramica completa sulla disciplina si rimanda comunque al già citato P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione europea*, cit. (capitolo 4, in cui si propone un puntuale commento della proposta di direttiva, ancora *in itinere*); G. CASSANO, M. AQUINO, *Il trattamento dei dati personali alla luce della direttiva 2002/58,* in *I Contratti*, 2003, pp. 402-412.

[300] Art. 5.

[301] Art. 4.

[302] Relazione introduttiva (COM(2000) 385), § 3.

Nonostante i significativi passi avanti, tuttavia, non si possono trascurare i limiti di questa impostazione, soprattutto per quanto riguarda le materie escluse e i regimi di eccezione.

Come ricordato, il principio posto a fondamento dell'architettura normativa mira a proteggere la riservatezza delle comunicazioni vietando ogni indebita interferenza. Trattandosi però di una disciplina riconducibile alle competenze del c.d. primo pilastro, anche in questo caso, le attività regolate dai titoli V e VI del trattato sull'Unione, come quelle relative alla sicurezza pubblica, la difesa, la sicurezza dello Stato e alla sfera del diritto penale in generale, non sono ricomprese nell'ambito di applicazione della dir. 2002/58[303].

In questi ambiti, dunque, gli Stati membri sono liberi di ammettere l'intercettazione dei contenuti delle comunicazioni secondo quanto previsto dal diritto nazionale e di imporre così ai fornitori del servizio particolari obblighi di conservazione e accesso ai dati di traffico e ubicazione[304].

Il Consiglio europeo, invero, aveva comunque adottato delle misure volte ad assicurare dei livelli di tutela minimi anche per le attività di trattamento dei dati riconducibili all'allora terzo pilastro. Tuttavia, proprio in occasione di questa riforma, il Gruppo Articolo 29 ha colto l'occasione per fare delle ulteriori sottolineature sui pericoli legati allo sviluppo delle tecnologie per l'integrità della sfera privata delle persone, soprattutto in ambiti così delicati come le comunicazioni[305].

---

[303] Art. 1, § 3

[304] Art. 15.

[305] Considerazioni critiche erano state già espresse con la *Raccomandazione n. 22/99 del 3 maggio 1999, relativa al rispetto della vita privata nel contesto dell'intercettazione delle telecomunicazioni* (WP 18) in risposta alla Risoluzione del Consiglio UE (spec. §§ 3 e 4). In particolare, erano state oggetto di perplessità le misure imponibili per la conservazione dei dati di traffico e, più ancora, dei dati relativi all'ubicazione dei dispositivi; contenuti certo non generati volontariamente dall'utente, eppure in grado di descriverne dettagliatamente aspetti molto puntuali delle vita privata, come la rete di relazioni e gli spostamenti.

Se per le intercettazioni telefoniche, infatti, la giurisprudenza di Strasburgo aveva elaborato negli anni una solida dottrina[306], rispetto alla conservazione dei dati di traffico e di localizzazione si intuivano maggiori rischi, in parte inediti rispetto al passato. Con il passaggio alle reti digitali, infatti, sarebbe stato possibile raccogliere una quantità di dati di gran lunga superiore a quel che si era potuto fare fino ad allora. Inoltre, un accesso indiscriminato a simili elementi – anche quando giustificato da ragioni di sicurezza e pubblico interesse – avrebbe permesso alle pubbliche autorità di ottenere facilmente una miriade di informazioni sulla vita privata dei singoli, fino a delineare i tratti di una «società controllata» (*surveillance society*).

Pur riconoscendo le potenzialità legate all'utilizzo di una così vasta gamma di contenuti, richiamando i principi già sanciti in altri ambiti, veniva ribadita l'opportunità di vietare misure di sorveglianza di portata generale e di limitare la conservazione dei dati solo nei limiti di quanto strettamente necessario, in linea con gli ideali di libertà propri di una società democratica.

### *d. La direttiva 2006/24*

I problemi appena accennati sarebbero però riemersi di lì a pochi anni. Il 25 marzo 2004, a seguito degli attentati terroristici di Madrid, il Consiglio europeo ha adottato una dichiarazione sulla lotta al terrorismo[307], in cui, alla luce dei recenti attacchi, si incoraggiava l'adozione di nuove misure per la conservazione dei dati di traffico onde favorire le attività di indagine e repressione di questo tipo di reati.

---

306 Si vedano, *ex multis,* le sentt. Kopp c. Svizzera, 25 marzo 1998; McLeod c. Regno Unito, 23 settembre 1998; Natoli c. Italia, 9 gennaio 2001; Jordachi c. Moldavia, 10 febbraio 2009, sentenza M.M. c/o Paesi Bassi; P.G. e J.H c/o Regno Unito; Lambert c/o Francia; Zakharov c/o Russia.

307 Consiglio europeo, *Dichiarazione sulla lotta al terrorismo*, 25 marzo 2004.

Un tentativo in tal senso si era già fatto in precedenza, nell'ambito del primo pacchetto di misure sulla protezione dei dati personali[308]. Tuttavia, i trattamenti riconducibili alla c.d. *data retention* si intersecavano con diverse materie relative alla cooperazione giudiziaria e di polizia in materia penale; un settore strettamente legato alle prerogative e alla sovranità dei singoli Stati[309].

Considerato l'enorme quantità di informazioni trattate dalle autorità nazionali nello svolgimento delle mansioni interne, così come nelle varie attività di cooperazione a livello comunitario (dalle politiche di asilo e immigrazione, al contrasto alla criminalità organizzata nelle sue diverse forme) la disciplina sulla protezione dei dati personali certo non era estranea a questo tipo di pratiche. Tuttavia, fermi alcuni principi ormai consolidati a livello europeo (*i.e.* sicurezza dei dati), il quadro normativo in quest'ambito si è delineato secondo logiche e regole in parte diverse da quelle generalmente previste dalla direttiva madre[310].

Fino a quel momento, i diversi Stati avevano adottato diverse misure di *data retention*, ognuno in deroga ai principi della dir. 2002/58 secondo le diverse

---

[308] Nella prima proposta della Commissione in merito al primo pacchetto sulla protezione dei dati personali, si alludeva al fatto che, «sul piano interno, oltre ad una direttiva-quadro […] si propone[sse] un insieme di altre misure complementari volte a garantire una protezione per quanto possibile completa» e per questo, «in tale ottica, una risoluzione dei rappresentati dei governi degli Stati membri riuniti in sede di Consiglio e una dichiarazione della Commissione [avrebbero] avuto per oggetto di rendere applicabili i principi della direttiva agli archivi che non rientrano nel suo campo di applicazione» COM(90) 314 def., p. 7, con riferimento al un progetto di risoluzione dei rappresenti dei governi degli Stati membri delle Comunità europee riunite in sede di Consiglio.

[309] Per questo motivo, le iniziative relative a quest'ambito erano sottoposte a procedure ben diverse da quelle proprie del diritto comunitario, lavorando, invece, secondo una logica di cooperazione tra i singoli governi, volto a conseguire l'unanimità in seno al Consiglio (c.d. metodo intergovernativo).

[310] A definire una sorta di cornice valoriale per l'utilizzo dei dati per finalità di prevenzione e repressione penale, inizialmente era stata una raccomandazione del Comitato dei Ministri del Consiglio europeo del 1987, cui poi erano seguite *l'acquis* di Schengen e, in seguito, il disciplinare previsto con la costituzione di Europol. Il punto di riferimento dei sistemi di tutela istituti attraverso tali accordi era costituito soprattutto ai canoni definiti dalla Convezione di Strasburgo, prevendendo come principi minimi la sicurezza e la riservatezza dei dati trattati e riconoscendo essenziali i diritti accesso e rettifica, come intesi in seno all'ordinamento della Cedu.

sensibilità[311]; una situazione che, col tempo, era risultata problematica almeno sotto tre punti di vista.

Innanzitutto, sul versante della *sicurezza*, un simile *patchwork* normativo si contrapponeva al rafforzamento della cooperazione giudiziaria ed investigativa in materia penale. La conservazione di dati diversi per periodi diversi, infatti, non solo costituiva un ostacolo alla definizione di uno standard comune, ma poteva incoraggiare un utilizzo "selettivo" dei mezzi di comunicazione, convogliando le attività criminali verso i sistemi sottoposti ad una disciplina più mite[312].

In secondo luogo, l'imposizione di obblighi disomogenei moltiplicava i *costi* in capo ai fornitori di servizi[313]. Questi ultimi, infatti, a tali condizioni, dovendo comunque garantire un adeguato livello di protezione dei dati conservati[314], si trovavano onerati di obblighi diversi in ciascuna giurisdizione, frenando così gli effetti delle politiche volte a favorire la concorrenza e il mercato interno[315].

Infine, l'archiviazione di una così vasta quantità di informazioni, costituiva *una forte ingerenza nei diritti* alla *privacy* e alla protezione dei dati personali; e ciò ancor prima di un eventuale accesso da parte delle autorità pubbliche. Le misure nazionali

---

311 Tale facoltà era stata esplicitamente prevista dall'art. 15, dir. 2002/58. A distanza di qualche anno, tuttavia, si era osservato come nell'esercizio delle proprie prerogative i legislatori nazionali si fossero orientati verso soluzioni assai diverse tra loro, così come emerge da: C. COCQ, F. GALLI, *Comparative law paper on data retention regulation in sample of EU Member States* (SURVEILLE – Surveillance: Ethical Issues, Legal Limitations, and Efficiency Collaborative Project; Deliverable 4.3) 30 aprile 2013, p. 13 ss.

312 Una della opzioni considerate anche a livello europeo, infatti, prevedeva l'ipotesi di limitare al conservazione ai soli dati già trattati nell'ambito di erogazione dei servizi, senza definire uno *standard* comune. Tuttavia, si era osservato come una simile scelta avrebbe potuto dirottare le attività criminose verso quei servizi meno interessati alla conservazione di tali informazioni, vanificando l'utilità della misura (rif. Consiglio dell'UE, *Progetto di decisione quadro sulla conservazione dei dati trattati e memorizzati nel quadro della fornitura di servizi di comunicazioni elettroniche accessibili al pubblico o dei dati sulle reti pubbliche di comunicazione a fini di prevenzione, ricerca, accertamento e perseguimento della criminalità e dei reati, compreso il terrorismo*, doc. 15098/04, 23 novembre 2004).

313 Dir. 2006/24, *considerando* nn. 5 e 6.

314 Dir. 2006/24, art. 7.

315 Un obiettivo che, per quanto documentato al tempo dell'adozione dell'atto, risulta ancora ben lontano da raggiungere, come rappresentano i dati in seguito emersi nella relazione della Commissione al Consiglio e al Parlamento europeo, *Valutazioni dell'applicazione della Direttiva sulla conservazione dei dati (Direttiva 2006/24/CE),* COM (2011), 28 ss.

infatti finivano con il vanificare gli obblighi di non tracciabilità previsti dalla dir. 2002/58, facendo di un'eccezione la normalità[316]; e tutto questo, evidentemente, in aperto contrasto non solo la tradizionale normativa europea sulla *privacy*[317], ma anche con quanto sancito dalla Carta di Nizza[318].

Nonostante la problematicità delle questioni sottese a questo genere di iniziative, la decisione del marzo 2004, dunque, mirava a promuovere l'adozione di uno strumento di armonizzazione in questo settore.

Il Trattato di Maastricht aveva incluso la cooperazione giudiziaria in materia penale nell'ambito delle competenze dell'Unione, ammettendo la possibilità di regolare questi ambiti, seppur dovendo ricorrere al tradizionale metodo intergovernativo[319]. Onde evitare però che di fronte all'alternativa tra diverse basi giuridiche si verificasse un ritorno alle procedure tipiche del diritto internazionale, l'art. 47 TUE aveva riconosciuto una *primauté* a favore del metodo comunitario[320], favorendo così indirettamente l'esercizio delle competenze del primo pilastro.

La *data retention* si è presentata dunque come una materia delle sfaccettature poliedriche; una sorta di competenza "interpilastro" a metà strada tra le misure a tutela del mercato e quelle a presidio della sicurezza nazionale[321].

---

316 Dir. 2006/24, *Considerando* nn. 3 e, specificamente, art. 3 in deroga a quanto previsto dalla dir. 2002/58, artt. 5, 6 e 9.

317 F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 128-130. Come l'Autore infatti sottolinea, non solo la formulazione del diritto alla *privacy* e alla protezione dei dati personali ha costituito un'attuazione molto evolutiva di quanto previsto dall'art. 8 della CEDU, ma, ben prima del Trattato di Lisbona, la dir. 95/46 ne aveva sancito una tutela completa (così come, peraltro, confermato anche dalla CGUE nella sent. 24 novembre 2011, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) / Administración del Estado*, cause riunite C-468/10, C-469/10, par. 28-29).

318 T. GROPPI, *Art. 7*, e F. DONATI, *Art. 8*, in R. BIFULCO, M. CARTABIA, A. CELOTTO (a cura di), *L'Europa dei diritti*, cit.; G. TIBERI, *Riservatezza e protezione dei dati personali*, in M. CARTABIA (a cura di), *I diritti in azione*, cit., 368 ss.

319 *Ex multis*, L. DANIELE, *Diritto dell'Unione europea*, Torino, 2014, 226 ss.

320 Più diffusamente, sul punto si rimanda a R. MASTROIANNI, *Art. 47 TUE*, in TIZZANO (a cura di), *Trattati dell'Unione europea e della Comunità europea*, Milano, 2004, 167.

321 L PALADINI, *I conflitti fra pilastri dell'Unione europea e le prospettive del Trattato di Lisbona*, in *Il Diritto dell'Unione europea*, 2010, 87-90, 102-105; F. FONTANELLI, *La Corte di Giustizia e il "favor*

Per questo motivo, il 28 aprile 2004, i governi di Francia, Irlanda, Svezia e Regno Unito, per introdurre le nuove misure di contrasto, avevano presentato una proposta di decisione quadro, facendo leva su quanto previsto dagli artt. 31, n. 1, lett. *c*) e 34, n. 2, lett. *b*) TUE, nell'ambito delle competenze *ex* terzo pilastro[322]. Tale proposta tuttavia, dopo aver ricevuto pensanti critiche, fu presto cassata, preferendo orientarsi verso l'adozione di una direttiva ancorata alle previsioni dell'art. 95 CE, abbracciando una prospettiva *market-oriented*[323].

In accordo con la base giuridica scelta, la portata di questa nuova normativa fu circoscritta alla sola armonizzazione degli obblighi imposti agli operatori[324], uniformando le categorie di dati trattati[325] e riducendo la discrezionalità sui tempi di conservazione[326].

Uno degli aspetti più rilevanti della nuova disciplina però riguardava la natura delle prescrizioni rivolte agli Stati, radicalmente diverse da quanto previsto in precedenza dall'art. 15 della direttiva 2002/58[327]. Tale norma, infatti, permette di

---

*communitatis". Il percorso della giurisprudenza della Corte di Giustizia delle Comunità europee sul fondamento normativo degli atti dell'Unione*, in *Rivista italiana di diritto pubblico comunitario*, 2010.

[322] Nello specifico, un progetto presentato dal Francia, Inghilterra, Regno Unito e Irlanda, *Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detect*, doc. 8958/04, 20 dicembre 2004.

[323] Consiglio dell'UE, *Progetto di decisione quadro sulla conservazione dei dati trattati e memorizzati nel quadro della fornitura di servizi di comunicazioni elettroniche accessibili al pubblico o dei dati sulle reti pubbliche di comunicazione a fini di prevenzione, ricerca, accertamento e perseguimento della criminalità e dei reati, compreso il terrorismo - Base giuridica*, doc. 7688/05, 5 aprile 2005, spec. 2–7.

[324] Dir. 2006/24, art. 3, includendo – peraltro in termini tutt'altro che restrittivi – i dati necessari per rintracciare e per identificare le fonte e la destinazione di una comunicazione, così da stabilirne la natura, la data, l'ora e la durata, l'ubicazione degli utenti e il tipo di strumentazione utilizzata.

[325] Dir. 2006/24, art. 5.

[326] Dir. 2006/24, art. 6.

[327] Dir. 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (dir. relativa alla vita privata e alle comunicazioni elettroniche). È nell'adozione di questa direttiva che si avverte per la prima volta il mutato clima del *post* 11 settembre. A differenza della dir. 95/46, infatti, la "novella" del 2002, alla luce degli avvenimenti dell'anno prima, stempera i toni garantisti, limitando tuttavia la possibilità della *data retention* ad una mera facoltà rimessa al legislatore. Sarà solo la dir. 2006/24, dopo i fatti di Madrid e Londra, a cambiare definitivamente la

derogare alle ordinarie garanzie per la tutela della *privacy* "elettronica", solo in casi particolari (quali appunto – tra i vari – la sicurezza nazionale, la difesa, e il contrasto di reati gravi) ammettendo la sospensione del normale obbligo di cancellazione dei metadati a patto che vengano comunque rispettati i limiti imposti dal diritto comunitario[328].

Quella che fino a quel momento era stata considerata una mera *facoltà*[329], , con la dir. 2006/24 si trasformava così in un *obbligo*[330], imponendo l'utilizzo di questi strumenti come un normale metodo investigativo per la repressione di gravi reati. E nel disporre in tal senso, l'atto si è limitato a considerare principalmente i profili inerenti la portata degli adempimenti privati, delegando ai singoli Governi la definizione dei presupposti e delle garanzie relative all'accesso da parte delle pubbliche autorità[331].

Questa scelta, sebbene inizialmente avvalorata dalla Corte di Giustizia[332], ha però continuato a destare pesanti critiche[333]. La normativa, infatti, aveva imposto

---

rotta, trasformando un'eventuale eccezione in obbligo. (v. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 129; A. VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto. La "data retention" al test di legittimità*, cit., 1229).

328 Dir. 2002/58, art. 15, par. 1, ultimo periodo: «Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea.». Norma che, in definitiva, andava ad includere anche i principi inerenti la tutela dei diritti fondamentali così come previsi, dapprima, dalla CEDU e dalla tradizione costituzionale degli Stati membri e, in seguito, dalla Carta di Nizza.

329 Dir. 2002/58, art. 15, par. 1, primo periodo, in cui si legge «gli Stati membri *possono* adottare disposizioni legislative volte a limitare i diritti e gli obblighi…».

330 Dir. 2006/24, art. 3, par. 1, in cui diventa: «In deroga agli articoli 5, 6 e 9 della Direttiva 2002/58/CE, gli Stati membri *adottano* misure per garantire che i dati […] siano conservati conformemente alle disposizioni della presente Direttiva».

331 Dir. 2006/24, art. 4.

332 Sent. 10 febbraio 2009, *Irlanda/Parlamento e Consiglio*, causa C-301/06, in cui la Corte ha confermato la scelta della base giuridica osservando come la disciplina, limitandosi ai profili privatistici e vincolando la portata delle misure al rispetto del diritto comunitario, potesse (e dovesse: par. 78) essere adottata sui presupposti dell'art. 95 CE. F. FONTANELLI, *La Corte di Giustizia e il "favor communitatis"*, cit.

333 F. BIGNAMI, *Protecting Privacy Against the Police in the European Union : The Data Retention Directive*, in Y. BOT (a cura di), *Melanges en l'Honneur de Philippe Leger: le droit a la mesure de l'homme*, Parigi, 2006; ID., *Privacy and Law Enforcement in the European Union: the Data Retention Directive*, in *Chigago Journal of International Law*, 2007; L. FEILER, *The Legality of the Data Retention Directive in Light of*

degli obblighi destinati a comportare una grave compromissione della *privacy,* imponendo un trattamento massivo dei dati senza definire contestualmente un adeguato sistema di garanzie. Il testo, a riguardo, non si era spinto oltre a dei meri richiami al rispetto dei diritti in questione [334] con dei cenni assolutamente insufficienti a compensare le limitazioni introdotte (soprattutto alla luce di quanto stabilito dalla Carta di Nizza)[335].

Per questi motivi, la dir. 2006/24 è stata oggetto di un acceso dibattito. Fin dall'inizio, se la Commissione, da un lato, aveva sanzionato severamente i legislatori inadempienti al recepimento[336], dall'altro, le Corti nazionali avevano dichiarato l'illegittimità costituzionale della disciplina di attuazione[337]. Nel susseguirsi delle

---

*the Fundamental Rights to Privacy and Data Protection*, in *EJLT*, 2010; E. KOSTA, *The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Protection Directive with the Rights to Privacy and Data Protection*, in *Scripted*, 2013.

[334] Dir. 2006/24, art. 4, ultimo periodo, in cui si legge: «Le procedure da seguire e le condizioni da rispettare per avere accesso ai dati conservati in conformità dei criteri di necessità e di proporzionalità sono definite da ogni Stato membro nella legislazione nazionale, con riserva delle disposizioni in materia del diritto dell'Unione europea o del diritto pubblico internazionale e in particolare della CEDU, secondo l'interpretazione della Corte europea dei diritti dell'uomo.»

[335] Anche il mero riferimento all'esigenza di includere le previsioni nella legislazione nazionale, senza soffermarsi sulle caratteristiche minime dell'atto di recepimento, è stato oggetto di analisi. Nella ricostruzione offerta dell'AG nel caso *Tele2 Sverige*, infatti, anche la sola individuazione di una corretta base giuridica risulta problematica, a fronte del fatto che lo stesso significato della parola "legge" o di locuzioni tipo "misura legislativa" può assumere un significato diverso nei singoli contesti nazionali, individuando fonti con un diverso grado di specificità e vincolatività (*Tele2 Sverige*, Conclusioni AG, par. 144 ss.)

[336] Sent. 26 novembre 2009, *Commissione/Grecia*, causa C-211/09; Sent. 26 novembre 2009, *Commissione/Irlanda*, causa C-202/09; sent. 4 febbraio 2010, *Commissione/Svezia*, causa C-185/09; sent. 29 luglio 2010, *Commissione/Austria*, causa C-189/2009. In particolare, inoltre, va ricordata un'ulteriore procedura che, in seguito, ha visto coinvolta nuovamente la Svezia, condannata al pagamento di una somma forfettaria di 3 milioni di euro (sent. 30 maggio 2013, *Commissione/Svezia*, causa C-270/2011).

[337] Si erano, infatti, pronunciate nel frattempo la Corte suprema amministrativa bulgara (2008); la Corte suprema rumena (2009); il Tribunale costituzionale federale tedesco (2009); la Corte suprema cipriota (2011) e la Corte costituzionale ceca (2011); senza contare i ricorsi pendenti al momento del rinvio alla CGUE, avanti la Corte costituzionale polacca (2011) e la Corte costituzionale slovacca (2012). In dottrina si rimanda a E. KOSTA, *The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Protection Directive with the Rights to Privacy and Data Protection*, cit.; J. DURICA, *Directive on the Retention of Data on Electronic Communication in the Rulings of the Constitutional Courts of the EU Member States and Efforts for its Renewed Implementation*, *TQL*, 2013; A.

diverse pronunce, dunque, la complessa natura della disciplina è stata messa più volte in forte discussione. Si è avvertita così l'esigenza di ridefinire i valori in gioco, non più limitandosi a considerare i meri interessi economici della prima ora, ma estendendo l'analisi anche ai profili fino a quel momento trascurati–*in primis* la tutela dei diritti.

La Corte di giustizia, dunque, finalmente interpellata dalla Corte costituzionale austriaca e dalla Corte suprema irlandese, nel 2012, con la sentenza *Digital Rights Ireland*, ha colto l'occasione per rispondere alla numerose perplessità emerse fino ad allora, fino ad arrivare a dichiarare l'invalidità dell'intera direttiva. Sulla portata di questa decisione, tuttavia, ci sarà modo di tornare meglio in seguito.

### *2.3. Verso la costituzionalizzazione della protezione dei dati personali a livello europeo*

Al termine di questa breve panoramica, è necessario un momento di sintesi. Passando in rassegna i contenuti delle varie normative, infatti, a più riprese sono affiorati temi e questioni che caratterizzano la disciplina che qui ci occupa e che hanno segnato il passo nell'evoluzione del diritto comunitario su questi temi.

Riprendendo le tre categorie di problemi accennate all'inizio, si possono quindi trarre delle prime considerazioni.

In primo luogo, da un punto di vista strettamente tecnico, spiccano i problemi legati al rapido sviluppo della componente tecnologica. Trovandosi di fronte ad un oggetto materiale per sua natura estremamente mutevole, il legislatore infatti comunemente incontra non poche fatiche nell'inquadrare definizioni e concetti. L'utilità della norma si gioca soprattutto sulla sua capacità di adattarsi ai diversi sviluppi, creando però nuove tensioni quanto alla certezza dei diritti e alla certezza

---

VEDASCHI, V. LUBELLO, *Data Retention and its Implications for the Fundamental Right to Privacy*, *Tilburg L. Rev.*, 2015, 22–26.

del diritto. La tecnica normativa dunque evolve, ragionando soprattutto per principi e creando poi riferimenti e luoghi per promuovere la coerenza nel naturale dinamismo dell'interpretazione.

In secondo luogo, guardando specificamente alla natura del diritto europeo, si sono colti in modo chiaro i limiti legati alla specificità delle basi giuridiche cui tradizionalmente si è ancorata la *data protection*. In linea con gli obiettivi e i fini di quest'ordinamento, il punto di partenza non poteva non essere la tutela del mercato; e questo nonostante la natura trasversale dell'informatizzazione e la pluralità degli interessi coinvolti nella c.d. società dell'informazione. Con l'andare del tempo, tuttavia, sono affiorate in modo evidente le contraddizioni che discendono a quest'approccio, mettendo in luce le forzature cui questo conduce (basti pensare ai problemi incontrati rispetto alla disciplina sulla *data retention*). Da più parti, quindi, si sono cominciati a cercare i presupposti per poter disporre di una base d'azione più ampia, in linea con i risultati raggiunti nel corso del processo di integrazione europea anche e soprattutto rispetto alla tutela dei diritti.

Ricollegandosi a quest'ultimo punto, emergono infine le questioni relative all'oggetto di tutela, ossia la protezione dei dati personali. Come si è già avuto modo di ricordare, si tratta di un presidio giuridico di natura complessa, che intercetta una pluralità di interessi che solo in parte possono essere ascritti ai valori della riservatezza. E quest'elemento trasversale è particolarmente accentuato dal crescente sviluppo di tecnologie legate proprio alla produzione e all'elaborazione dei dati. Aumentando infatti la quantità di informazioni e i campi e gli ambiti che attraverso i diversi contenuti possono essere rappresentati, il perimetro dei relativi istituti di tutela spesso va ad espandersi, facendo della protezione dei dati personali, un presidio che tende ad affrancarsi da una funzione strumentale soltanto ai valori della *privacy*; un diritto presupposto per la tutela di *tutti* i diritti fondamentali intercettati dalla digitalizzazione.

Alla luce di queste considerazioni, dunque, si cominciano a cogliere le ragioni che hanno indotto il legislatore europeo a conferire uno spazio privilegiato a questa materia. Come osservato, si tratta di un insieme di discipline particolarmente significative nella storia dell'integrazione europea, e che in prospettiva avranno un ruolo sempre più cruciale nel tutelare gli interessi degli Stati membri e dei cittadini dell'Unione. Sulla base di queste premesse, dunque, nelle prossime pagine si prenderanno in esame i passaggi che hanno portato al pieno riconoscimento di un diritto fondamentale alla protezione dei dati personali e al rafforzamento delle competenze europee in quest'ambito.

### 3. La protezione dei dati personali come diritto fondamentale dell'UE

Muovendo da quanto accennato nei paragrafi precedenti, a questo punto, va dedicata particolare attenzione alle coordinate istituzionali che hanno consolidato il valore costituzionale del diritto alla protezione dei dati personali a livello europeo (art. 8 CDFUE), nonché il riconoscimento di una competenza generale a favore dell'Unione nel regolamentare i settori inerenti a questa materia (art. 16 TFUE).

Come ricordato, questo percorso inizia con i lavori preparatori per un *bill of rights* comunitario; un progetto che ha cominciato a farsi strada a metà degli anni Settanta[338] e poi culminato, nel 2000, con l'approvazione della Carta di Nizza[339].

---

[338] Nonostante la Corte di giustizia delle Comunità europee inizialmente avesse adottato un orientamento defilato rispetto alle questioni inerenti la compatibilità tra diritto comunitario e diritti fondamentali, con il tempo, anche a fronte delle sollecitazioni da parte dei Giudici e delle Corti nazionali, ha ammesso alcune aperture (inizialmente, sono state paradigmatiche, in tal senso, le pronunce relative alle cause *Stauder* (cit.)*, Internationale Handelsgesellschaft* (sent. 17 dicembre 1970, C-11/70)e *Nold II* (sent. 14 maggio 1974, C-4/73)). In particolare, come ci sarà modo di vedere meglio in seguito, alcune Corti costituzionali (soprattutto la Corte Federale tedesca) non avevano mancato di sottolineare la sostanziale inadeguatezza della legislazione comunitaria sul punto, evidenziando come, fintanto che non fossero state colmate tali lacune, non vi sarebbe potuta essere una piena accettazione della *primauté communautaire.* In ragion di ciò, dunque, già nel 1975 la

Si tratta di un itinerario lungo e tortuoso, che ha visto emergere non poche tensioni nei rapporti tra le istituzioni di Bruxelles e gli Stati membri, soprattutto per quanto riguarda le questioni inerenti la protezione dei dati personali.

L'intento, dunque, è quello di analizzare le evoluzioni che hanno portato a questa concentrazione in sede europea delle competenze e della disciplina sulla *data protection*, mettendo in luce i presupposti e le ragioni che oggi spingono verso l'elaborazione di una strategia di *data governance* comune.

### *3.1. Premessa: la tutela dei diritti fondamentali nell'ordinamento comunitario*

Come anticipato, le principali basi giuridiche su cui oggi poggia il diritto alla protezione dei dati personali nell'ordinamento europeo sono individuate dall'art. 8 CDFUE e dall'art. 16 TFUE. Tuttavia, prima di dedicarsi all'analisi di tali norme è necessario fare una breve una premessa sull'evoluzione del sistema di tutela dei diritti nell'ordinamento comunitario.

---

Commissione europea aveva promosso un primo studio sulla possibilità di elaborare un catalogo dei diritti fondamentali da includere nel diritto dei Trattati (Cfr. Commissione delle Comunità europee, *Rapporto sull'Unione Europea*, in *Gazzetta Ufficiale delle Comunità europee*, 5/75). A partire da quei primi lavori, nel 2001 la Convenzione di Nizza avrebbe approvato la Carta dei diritti fondamentali dell'Unione europea, riconosciuta a tutti gli effetti come fonte di diritto primario nel 2009, in seguito a quanto previsto dal Trattato di Lisbona.

[339] Oltre ad aver riconosciuto il ruolo di fonte di diritto primario alla Carta di Nizza, il Trattato di Lisbona, riferendosi a quanto in precedenza previsto dall'art. 286 TCE in seguito alle modifiche apportate dal Trattato di Amsterdam, ha riconosciuto al Parlamento e al Consiglio europeo una competenza di carattere generale a disciplinare le materie inerenti la protezione dei dati personali. L'art. 16 TFUE – come si vedrà in questo paragrafo – prevede che: «ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. (§ 1). Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale 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, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea. (§ 2)».

Inizialmente, infatti, non si pensava che le nascenti Comunità europee si sarebbero occupate di diritti fondamentali[340] in quanto, originariamente, il progetto era stato concepito soprattutto come una realtà economica e non come un vero e proprio sistema politico. Si era ritenuto più opportuno, quindi, che della tutela dei *diritti* continuassero a farsi carico le Costituzioni e la legislazione dei singoli Stati[341], lasciando alle Autorità sovrannazionali e la Corte di giustizia il solo compito di promuovere le *libertà* necessarie alla realizzazione del mercato comune[342].

Si trattava di scelta assolutamente deliberata, dal momento che, soprattutto nel secondo dopoguerra, il tema dei diritti fondamentali aveva avuto ovunque una forte eco[343]. Pensando al nascente ordinamento comunitario, i lavori preparatori alla Cedu, infatti, avevano messo in luce come, pur esistendo un solido substrato culturale – condiviso non solo dagli Stati membri ma, più in generale, da diversi gli

---

[340] J.H.H. WEILER, *Il sistema comunitario europeo. Struttura giuridica e processo politico,* Bologna, Il Mulino, 1985, pp. 141 ss.; M. CARTABIA, *L'ora dei diritti fondamentali nell'Unione europea*, in ID. (a cura di), *I diritti in azione*, cit., pp. 15 ss.; D. BUTTURINI, *La tutela dei diritti fondamentali nell'ordinamento costituzionale italiano ed europeo*, Napoli, Editoriale Scientifica Italiana, 2009, pp. 3 ss. In molti, infatti, avevano osservato come la tutela dei diritti fondamentali rappresentasse una componente essenziale degli ordinamenti "politici" che non dei sistemi "economici", come quelli istituti dai Trattati.

[341] In molti, infatti, avevano osservato come la tutela dei diritti fondamentali rappresentasse una componente essenziale degli ordinamenti "politici" che non dei sistemi "economici", come quelli istituti dai Trattati. P. GREMENTIERI, *Il processo comunitario. Principi e garanzie fondamentali*, Milano, Giuffrè, 1973, p. 24 ss.; M. LUCIANI, *Diritti sociali e integrazione europea*, in *Politica del diritto*, 2000, p. 367; A. MANZELLA, *Dal mercato ai diritti*, in A. MANZELLA, P. MELOGRANI, E. PACIOTTI, S. RODOTÀ (a cura di), *Riscrivere i diritti in Europa*, Bologna, Il Mulino, 2001, p. 29.

[342] I riferimenti sono alle previsioni contenute soprattutto nel Trattato CEE sulla libertà di circolazione delle merci (artt. 9 e 37), dei capitali (art. 67), dei lavoratori (art. 48), di prestazioni dei servizi (art. 59), di stabilimento (art. 52) e di concorrenza (art. 85).

[343] Come già ricordato, infatti, molti Stati avevano appena approvato nuove Carte costituzionali dedicando al tema dei diritti fondamentali particolare attenzione (paradigmatici gli esempi di Germania, Austria, Italia e Francia, come analizzati*, ex multis*, negli scritti dell'Associazione Italiana dei Costituzionalisti, *La nascita delle Costituzioni europee del secondo dopoguerra*, Padova, Cedam, 2000). Inoltre, a livello internazionale, se in seno alla Conferenza delle Nazioni Unite, alla fine del conflitto era stata proclamata la Dichiarazione universale dei diritti umani (1948), pochi anni più tardi, a Roma, il Consiglio d'Europa arrivava a siglare la già ricordata Convenzione europea per i diritti dell'uomo e del cittadino (1950). Un movimento che, considerato nel suo insieme, certo documenta la centralità del tema in quel periodo.

ordinamenti continentali – vi erano comunque delle marcate differenze tra i livelli di garanzia assicurati all'interno dei singoli contesti nazionali[344].

In particolare, l'ambito in cui erano emerse maggiori differenze era soprattutto quello dei diritti economici e sociali; la categoria più toccata dall'iniziative ora condivise a livello comunitario. Rispetto a questi ultimi era risultato difficile non solo individuare in modo univoco le fattispecie di interesse, ma anche definire gli adeguati standard di tutela, troppo spesso condizionati da profonde differenze economiche e culturali[345]. Per tali motivi, dunque, con l'intento di preservare il più possibile l'autonomia e l'identità economica dell'ordinamento comunitario, per evitare di comprimere l'azione europea in settori nevralgici, in materia di diritti fondamentali si preferì evitare ogni obbligo[346]. E in tal senso, non solo i Trattati avevano del tutto trascurato il tema, ma i giudici europei, nelle loro prime sentenze, si erano mostrati essenzialmente indifferenti rispetto ai diritti tutelati dalle Carte nazionali, escludendo categoricamente che tali disposizioni potessero mai costituire un parametro di legittimità per la normativa comunitaria[347].

---

[344] A riprova di quest'approccio, basti ricordare l'iniziale atteggiamento di *self-restraint* riscontrato nella prima giurisprudenza della Corte Edu e dell'ancor presente margine di discrezionalità concesso a favore degli Stati aderenti alla Convenzione rispetto all'obbligo di adeguare il diritto interno alle indicazioni ricavabili dalle diverse pronunce.

[345] M. CARTABIA, *L'ora dei diritti fondamentali nell'Unione europea*, in ID. (a cura di), *I diritti in azione*, cit., pp. 16-17 ss., con riferimento anche a quanto constatato in M.A. GLENDON*, I diritti nelle Costituzioni del ventesimo secolo*, in ID. (a cura di), *Tradizioni in subbuglio* (trad. it. a cura di P.G. Carozza e M. Cartabia), Soveria Mannelli, Rubettino, 2007.

[346] D. BUTTURINI, *La tutela dei diritti fondamentali nell'ordinamento costituzionale italiano ed europeo*, cit., pp. 3 ss. Paradigmatiche, in tal senso, le celeberrime sentenze *Stork* [CGCE, sent. 4 febbraio 1959, *Friesrich Stork et Co. c. Alta Autorità della CECA*, causa C-1/58]; *Geitling* del 1960 [CGCE, sent. 21 febbraio 1960, *Geitling et al. c. Alta Autorità della CECA*, cause riunite C-16, 17, 18/59] e *Sgarlata* del 1965 [CGCE, sent. 1 aprile 1965, *Avv. Marcello Sgarlata et al. c. Commissione*, causa C-40/65].

[347] Paradigmatiche, in tal senso, le celeberrime sentenze *Stork* [CGCE, sent. 4 febbraio 1959, *Friesrich Stork et Co. c. Alta Autorità della CECA*, causa C-1/58]; *Geitling* del 1960 [CGCE, sent. 21 febbraio 1960, *Geitling et al. c. Alta Autorità della CECA*, cause riunite C-16, 17, 18/59] e *Sgarlata* del 1965 [CGCE, sent. 1 aprile 1965, *Avv. Marcello Sgarlata et al. c. Commissione*, causa C-40/65].

Tuttavia, con l'affermazione del principio della c.d. *primauté communautaire*[348], di fronte alla pretesa di disapplicare il diritto nazionale a favore di quello europeo, i giudici e la dottrina costituzionale avevano dimostrato alcune perplessità. Un rafforzamento del ruolo del diritto comune negli ordinamenti interni, in assenza di adeguate garanzie a favore dei diritti fondamentali, infatti, per molti rappresentava una mancanza difficile da accettare, tant'è che, in alcuni casi, si è arrivati ad individuare le condizioni per sottrarsi al primato europeo (i c.d. *controlimiti*) per salvaguardare gli standard di tutela assicurati dal diritto costituzionale statale[349].

Per allentare le possibili tensioni generate da questo potenziale scontro tra Corti, a partire dalla fine degli anni Sessanta, il tema dei diritti fondamentali ha così gradualmente cominciato a farsi spazio anche nell'ordinamento comunitario.

I giudici lussemburghesi, infatti, a partire dalla sentenza *Stauder* hanno cominciato a dimostrare alcuni primi cenni di apertura su questo fronte[350], fino ad elaborare poi, nel tempo, una loro specifica dottrina. Dopo aver affermato che i diritti fondamentali sono parte integrante dei principi generali del diritto europeo[351], nella giurisprudenza comunitaria comincia a farsi strada un graduale riconoscimento

---

[348] Dapprima, infatti, la Corte, nella famosa sentenza *Van Gend en Loos* [CGCE, sent. 5 febbraio 1963, *Nv Algemene Transport – en expeditie onderneming Van Gen en Loos c. Amministrazione olandese delle imposte,* C-26/62], aveva sancito il principio dell'effetto diretto degli atti e della normativa comunitaria all'interno dei sistemi giuridici nazionali; in un'altra storica pronuncia, di poco successiva, nella causa *Costa c. Enel* [CGCE, sent. 15 luglio 1964, *Flaminio Costa c. Enel*, causa C-6/64] aveva riconosciuto il primato del diritto europeo sul quello interno.

[349] *Solange I*

[350] In dottrina, sul punto, J.H.H. WEILER, *Il sistema comunitario*, cit. p. 145 ss.; J.H.H. WEILER, *Eurocracy and Distrusts. Some Questions Concerning the Role of the European Court of Justice in the Protection of Fundamental Human Rights withtin the Legal Order of the European Communities*, in *Washington Law Review*, 1986, p. 1110; M. CARTABIA, *Principi involabili e integrazione europea*, Milano, Giuffrè, 1995, p. 24 ss.; R. BIFULCO, M. CARTABIA, A. CELOTTO, *Introduzione,* in IID. (a cura di), *L'Europa dei diritti*, Bologna, Il Mulino, 2001, pp. 13 ss.; G.F. FERRARI, *I diritti tra costituzionalismi statali e discipline transnazionali*, in ID. (a cura di) *I diritti fondamentali dopo la Carta di Nizza. Il costituzionalismo dei diritti*, Milano, Giuffrè, 2001, pp. 86 ss.; M. CARTABIA, *L'ora dei diritti fondamentali nell'Unione europea*, in ID. (a cura di), *I diritti in azione*, cit., pp. 18 ss.

[351] CGCE, sent. 12 novembre 1969, *Erich Stauder c. città di Ulm-Sozialamt* (causa C.29/69); in cui la Corte, pur non rilevando nella disposizione censurata (art. 189 Tratt. CEE) una possibile causa di violazione dei diritti fondamentali, afferma come questi facciano «parte dei principi generali del diritto comunitario, di cui la Comunità garantisce l'osservanza», *ex* art. 220 Tratt. CEE

delle relative garanzie, interpretate secondo un modello di protezione in linea con obiettivi dell'ordinamento comunitario[352]. La Corte, infatti, per individuare i propri parametri di legittimità, ha attinto dai contenuti delle diverse Carte individuando i principi comuni alla tradizione costituzionale degli Stati membri e alla Cedu[353], delineando però dei nuovi standard di protezione in funzione delle esigenze del diritto comune[354].

In parallelo, anche grazie a questi sviluppi, nello stesso periodo, in seno alla Commissione e al Parlamento europeo, ha poi cominciato a corroborarsi l'idea di addivenire ad un *bill of rights* comunitario[355]. Era ormai chiaro, infatti, che l'Unione

---

[352] CGCE, sent. 17 dicembre 1970, *Internationale Handelsgesellschaft mbH c. Einfuhr- und Vorratsstelle für Getreide und Futtermittel* (causa C- 11/70), in cui la Corte non si è determinata ad assumere le norme costituzionali degli Stati membri come parametro di legittimità degli atti di diritto comunitario, bensì assumendoli come *criteri interpretativi*. Come si legge, infatti: «Il richiamo a norme o nozioni di diritto nazionale nel valutare la legittimità di atti emananti dalle istituzioni della Comunità menomerebbe l'unità e l'efficacia del diritto comunitario. La validità di detti atti può essere stabilita unicamente alla luce del diritto comunitario. (§ 3) […] È tuttavia opportuno accertare se non sia stata violata alcuna garanzia analoga, inerente al diritto comunitario. La tutela dei diritti fondamentali costituisce infatti parte integrante dei principi giuridici generali di cui la Corte di giustizia garantisce l'osservanza. La salvaguardia di questi diritti, pur essendo informata alle tradizioni costituzionali comuni agli stati membri, va garantita entro l'ambito della struttura e della finalità della Comunità. (§ 4)»

[353] CGCE, sent. 14 maggio 1974, *J. Nold, Kohlen- und Baustoffgroßhandlung c. Commissione delle Comunità europee*, (causa C-4/73), in cui la Corte, richiamando quanto già affermato in *Stauder* e *Internationale Handelsgesellschaft*, conferma come le tradizioni costituzionali comuni rappresentino un punto di riferimento nell'elaborazione pretoria del catalogo dei diritti fondamentali comunitari. Si legge: «Come questa Coste ha già avuto occasione di affermare, i diritti fondamentali fanno già parte integrante dei principi generali del diritto, di cui essa garantisce l'osservanza. La Corte garantendo la tutela di tali diritti, *è tenuta ad ispirarsi* alle tradizioni costituzionali comuni agli Stati membri» (§ 13, corsivo aggiunto).

[354] CGUE, sent. 13 dicembre 1979, *Liselotte Hauer c. Land Rheinland-Pfalz* (causa C-44/79), in cui si legge come la Corte, richiamandosi ai casi *Nold* e *Internationale Handelsgesellschaft*, abbia chiarito come intenda utilizzare i riferimenti alle tradizioni costituzionali comuni agli Stati membri, ossia attraverso l'individuazione delle diverse figure attraverso un'analisi comparatistica cui segue la definizione di un diritto e di nuovi standards comunitari (§§ 14-15).

[355] In tal senso, un punto di svolta – è bene ricordare – si era avuto in seguito alle due pronunce occorse nel caso *Solange* (Cfr. sent. 29 maggio 1974, *Solange I* (BVerfGE 37, 217); sent. 22 ottobre 1986*, Solange II* (BverfGe 73, 339)). In quello occasioni, infatti, la Corte costituzionale federale tedesca, aveva paventato la possibilità di venir meno al principio di efficacia diretta e *primauté communitaire* proprio per le lacune riscontrate sul tema dei diritti fondamentali a livello comunitario; ragioni che avevano indotto sia la Corte sia le altre istituzioni europee a prendere

rappresentava a tutti gli effetti una realtà *sui generis*, diversa per funzioni e scopi sia dagli ordinamenti nazionali, sia dalle tradizionali organizzazioni internazionali. Questo era risultato particolarmente evidente soprattutto nel modo in cui la giurisprudenza aveva lasciato spazio alla tutela dei diritti, qui intesi, appunto, in relazione ai fini specifici del contesto entro cui venivano interpretati. Alla luce di queste considerazioni, dunque, si avvertiva l'esigenza di raggiungere presto un punto di sintesi, in grado di mettere in luce le peculiarità del sistema comunitario rispetto ai suoi "concorrenti".

Il percorso così avviato, seguendo un *iter* lungo e frammentato[356], arriverà ad un primo punto di approdo soltanto nel 2000, in occasione dell'approvazione della Carta di Nizza.

---

posizione a riguardo. La Commissione delle comunità europee, nel 1975, aveva quindi commissionato un primo *report* in merito alla possibilità di elaborare un catalogo dei diritti da allegare agli atti istitutivi comunitari (CCE, *Una sfida per l'Europa*, in *Gazzetta Ufficiale delle Comunità europee*, supplemento 1/76; noto anche come *Rapporto Tindemans*, prendendo il nome dal relatore). Sulla base degli esiti di quella prima iniziativa, l'anno successivo, nel 1976, era stato quindi condotto uno studio comparatistico, per analizzare meglio le criticità cui si andava incontro nell'intraprendere una simile opera di codificazione (CCE, *Relazione della Commissione sulla salvaguardia dei diritti fondamentali*, in *Gazzetta Ufficiale delle Comunità europee,* 5/76, COM(76) 37 def.). Un provvisorio approdo del processo così avviato si ha con la dichiarazione comune di Parlamento, Consiglio e Commissione sulla protezione dei diritti fondamentali e sul rispetto della Convenzione Edu; atto siglato il 5 aprile 1977 (in *Gazzetta Ufficiale delle Comunità europee,* 77/C 103/01).

[356] Come accennato, la Convenzione di Nizza, pur avendo approvato l'omonima Carta, aveva lasciato molte questioni in sospeso, e questo non solo per quanto concerne la tutela dei diritti fondamentali ma anche rispetto ad altri profili istituzionali legati alle competenze dell'Unione e degli Stati membri e al ruolo dei parlamenti nazionali.

Nella prospettiva di colmare tali lacune, si auspicava che il Consiglio europeo di Laeken del 2001 si facesse carico di intervenire il tal senso, continuando quanto fatto fino a quel momento e portando a compimento il processo avviato due anni prima a Colonia.

È proprio nelle more di questi sviluppi che, per la prima volta, in una dichiarazione ufficiale del Parlamento europeo si auspica che l'Unione possa addivenire quanto prima ad una riorganizzazione dei suoi atti istitutivi arrivando ad «un documento unico, chiaro e conciso [ossia una sorta di] Costituzione»[356]. Quest'ultimo concetto, pur apparendo soltanto quella volta in un documento ufficiale, sarà gravido di conseguenze.

Era di tutta evidenza che le materie rispetto alle quali si stava andando a decidere – il riparto di competenze, la tutela dei diritti fondamentali, il ruolo delle istituzioni nazionali nell'ambito delle procedure comunitarie – cadevano in pieno in quella che normalmente in cotesti più familiari si sarebbe identificata come «materia costituzionale». E negli anni a seguire ci sarebbe mossi proprio in questa direzione, fino ad arrivare, nel 2003, alla presentazione di un primo progetto per un

Come si legge dal preambolo del documento, in linea con le conclusioni del Consiglio UE, l'obiettivo principale di quest'iniziativa è quello di procedere ad un ricognizione più sistematica dei diritti fondamentali tutelati a livello europeo[357], rafforzandone i meccanismi di tutela «alla luce dell'evoluzione della società, del progresso sociale e degli sviluppi scientifici e tecnologici»[358]. Nonostante l'esplicito intento ricognitivo, la Convenzione che ha lavorato al documento, utilizzando questa leva, si è quindi dimostrata assai propensa ad esercitare una forte discrezionalità rispetto alla scelta dei diritti da includere, introducendo così una serie di novità che rappresentano oggi i tratti distintivi di questo documento[359] (*in primis* il qui discusso diritto alla protezione dei dati personali, sancito esplicitamente dall'art. 8 CDFUE).

---

*Trattato che adotta una Costituzione per l'Europa*. Avviato il procedimento di ratifica[356], tuttavia, in alcuni Stati i referendum popolari indetti per vagliare l'adesione alla nuova proposta avevano avuto esiti negativi, ragion per cui definitivamente abbandonata l'idea di un processo costituente europeo, optando per un «periodo di riflessione».

[357] I Consigli europei di Colonia e Tampere avevano insistito sul fatto che la Carta avesse un valore soltanto ricognitivo rispetto a quanto già emerso dalla giurisprudenza e dalla tradizione costituzionale comune agli Stati membri; un'indicazione che si rinviene fedelmente nel preambolo del documento, in cui si legge: «La presente Carta *riafferma*, nel rispetto delle competenze e dei compiti della Comunità e dell'Unione e del principio di sussidiarietà, i diritti derivanti in particolare dalle tradizioni costituzionali e dagli obblighi internazionali comuni agli Stati membri, dal trattato sull'Unione europea e dai trattati comunitari, dalla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, dalle carte sociali adottate dalla Comunità e dal Consiglio d'Europa, nonché i diritti riconosciuti dalla giurisprudenza della Corte di giustizia delle Comunità europee e da quella della Corte europea dei diritti dell'uomo» (corsivo aggiunto). A commento di queste scelte, si rimanda, in particolare a J.H.H. WEILER, *La Costituzione dell'Europa*, Bologna, Il Mulino, 1999, pp. 213 ss.; R. BIFULCO, M. CARTABIA, A. CELOTTO, *Introduzione,* in ID. (a cura di), *L'Europa dei diritti*, Bologna, Il Mulino, 2001, pp. 11-12 ss.; M. CARTABIA, *L'ora dei diritti fondamentali nell'Unione europea*, in ID. (a cura di), *I diritti in azione*, cit., pp. 31 ss.; L. AZZENA. *Prospettive della Carta europea dei diritti e ruolo della giurisprudenza*, in G.F. FERRARI (a cura di), *I diritti fondamentali dopo la Carta di Nizza*, cit., pp. 123 ss.

[358] Carta dei diritti fondamentali dell'Unione europea, *Preambolo,* § 4.

[359] Sull'apporto delle diverse tensioni – novative/conservative – si vedano: A. MANZELLA, *Dal mercato ai diritti*, in A. MANZELLA, P. MELOGRANI, E. PACIOTTI, S. RODOTÀ (a cura di), *Riscrivere i diritti in Europa*, Bologna, Il Mulino, 2001, pp. 32-34; E. PACIOTTI, *La Carta: i contenuti, gli autori*, *ibidem*, pp. 9 ss; A. PACE, *A che serve la Carta dei diritti fondamentali dell'Unione Europea? Appunti preliminari*, in *Giurisprudenza costituzionale*., 2001, pp. 196 ss.

Com'è noto, peraltro, questo nuovo *bill of rights* era stato inizialmente concepito come parte di un più ampio progetto costituzionale, poi naufragato a causa degli esiti negativi di alcuni referendum condotti a livello nazionale. Le riforme istituzionali avviate a Nizza verranno così portate avanti negli anni successivi in termini ben più modesti, fino a raggiungere un nuovo punto di equilibrio, nel 2007, con il Trattato di Lisbona.

Ed è solo in occasione di quest'ultimo che la Carta entrerà a far parte a tutti gli effetti delle fonti di diritto primario dell'Unione. Nel periodo che ha separato questi due momenti, infatti, il valore di tale documento è stato molto controverso. Se, per un verso, si riteneva che l'enunciazione dei diritti in un atto di tal sorta avesse senz'altro un valore politico rispetto ai diritti fondamentali tutelati a livello europeo, dall'altro, molti manifestavano un certo scetticismo nel riconoscergli pieno valore vincolante. L'intero processo di codificazione, infatti, era stato accompagnato da forti resistenze, dovute essenzialmente ai timori di veder rafforzati le competenze e il primato europeo a discapito del diritto e della cultura costituzionale nazionale.

Tutto questo traspare in modo evidente nella definizione dell'ambito di applicazione e della portata dei diritti così garantiti; punti rispetto ai quali si era stati particolarmente cauti[360]. Se da un parte si è stabilito che la Carta si sarebbe applicata a tutte le istituzioni comunitarie così come agli Stati membri nell'attuazione del diritto comunitario, dall'altra, questa non avrebbe attribuito all'Unione competenze ulteriori rispetto a quanto già in precedenza sancito dai Trattati, conservando lo *status quo*. Con una clausola generale, tuttavia, si era stabilito che la limitazione dei

---

[360] Il riferimento va, rispettivamente, agli artt. 51 e 52 della Carta di Nizza. A commento delle due norme, si rimanda in particolare a M. CARTABIA, *Art. 51 Ambito di applicazione*, in R. BIFULCO, M. CARTABIA, A. CELOTTO, *L'Europa dei diritti*, cit. pp. [344-351]; T. GROPPI, *Art. 52 Portata dei diritti garantiti*, *ibidem*, pp. [351-360]; J. ZILLER, *Articolo 51 – Ambito di applicazione*, in R. MASTROIANNI, A. ALLEGREZZA, O. RAZZOLINI, O. POLLICINO (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, cit., pp. [1044-057]; F. FERRARO, N. LAZZERINI, *Articolo 52 – Portata dei diritti garantiti*, *ibidem*, pp. [1062-1082]; P. GIANNITI, *La «comunitarizzazione» della «Carta» a seguito del Trattato di Lisbona*, in ID. (a cura di), *I diritti fondamentali nell'Unione Europea*, cit., pp. [357-393] spec. pp. 364 ss.

diritti sarebbe stata sottoposta ai principi di legalità, proporzionalità e necessarietà e che, pur riconoscendo alla Cedu un «significato particolare»[361] quale «fonte di ispirazione privilegiata»[362], il sistema della Carta avrebbe potuto concedere una protezione più estesa di quanto garantito dalla giurisprudenza di Strasburgo, indentificando in essa soltanto uno standard di riferimento minimo.

Alla luce di queste premesse, dunque, si può passare ad analizzare più attentamente le previsioni relative alla protezione dei dati personali; una delle principali peculiarità che, nel complesso, contraddistinguono la Carta.

### *3.2. La protezione dei dati personali come diritto fondamentale dell'UE*

La scelta di riconoscere un nuovo diritto fondamentale alla protezione dei dati personali, rappresenta forse una delle maggiori novità introdotte dalla Carta di Nizza. Prima di allora, infatti, nessun documento internazionale si era premurato di sancire uno specifico diritto fondamentale rispetto all'utilizzo di questo tipo di informazioni, riconducendo piuttosto tali garanzie alla tutela della sfera privata.

Chiaramente, come ricordato, uno dei principali obiettivi del legislatore europeo era quello di addivenire ad un documento in grado di assicurare un elevato livello di tutela dei diritti anche alla luce degli sviluppi scientifici e tecnologici; ragione che spiega, almeno in parte quest'interessante (seppur critica) novità.

Sebbene le tradizioni costituzionali nazionali non lasciassero intuire una chiara convergenza in tal senso[363], in precedenza si era già avuto modo di constatare come

---

[361] CGCE, sent. 15 maggio 1986, *Marguerite Johnston c. Chief Constable of the Royal Ulster Constabulary*, (causa 222/84) § 18; sent. 21 settembre 1989, *Hoechst AG c. Commissione delle Comunità europee* (cause riunite 46/87 e 227/88) § 13; sent. 18 giungo 1991, *Elliniki Radiophonia Tiléorassi AE c. Dimotiki Etairia Pliroforissis e Sotirios Kouvelas (ERT)* (causa C. 260/89) § 41.

[362] T. GROPPI, *Art. 52 Portata dei diritti garantiti*, cit., p. 357.

[363] Guardando al modo in cui tale materia aveva trovato spazio all'interno dei vari ordinamenti, non si poteva fare a meno di notare come, sebbene vi fossero dei valori di riferimento ormai ampiamente condivisi[363], di fatto, la collocazione delle garanzie sui dati personali all'interno

dalla tutela dei dati dipendessero importanti prerogative legate non soltanto agli obiettivi del primo pilastro, ma più in generale al perseguimento di diversi obiettivi di integrazione[364]. Per tale motivo, dunque, a più voci era stata avanzata l'ipotesi di affrancare la tutela dei dati dal rispetto della vita privata, portando definitivamente a compimento l'evoluzione storica che negli ultimi quarant'anni aveva interessato il diritto alla c.d. *information privacy*[365].

---

del quadro costituzionale di ciascuno risultasse profondamente eterogeneo. Come ricordato, infatti, un vero e proprio diritto *sui generis* alla protezione dei dati si poteva riscontrare soltanto in quegli Stati che avevano approvato o emendato la loro Costituzione dopo l'entrata in vigore della direttiva generale. In altri, certo, si erano ricondotte queste garanzie a diritti già codificati nel testo, riconoscendovi però soltanto una funzione strumentale e in altri ancora, la giurisprudenza costituzionale aveva incluso tali garanzie nel novero dei diritti fondamentali richiamandosi a principi assoluti come la dignità e la libertà umana. Tuttavia, in generale, in molti ordinamenti vi erano ancora situazioni di profonda incertezza circa la natura e i contenuti di questo diritto e ancor più sulla possibilità di attribuirgli chiaramente un'autonoma rilevanza sul piano costituzionale.

[364] Come ricordato, infatti, fin dalle sue prime pronunce in materia di diritti fondamentali, la Corte di giustizia avesse dimostrato un approccio inedito rispetto a questo tema, mettendo in luce l'autonomia e l'indipendenza dell'ordinamento comunitario. In particolare, nonostante i riferimenti alla tradizione costituzionale comune agli Stati membri, la giurisprudenza da prova che, da un punto di vista metodologico, non abbiano mai assunto norme di diritto interno come parametro di validità per gli atti di diritti comunitario, elaborando piuttosto *sulla base* di tali principi una serie di criteri propri, tagliati sulle esigenze e sulla ragion d'essere del diritto comunitario (Cfr. R. BIFULCO, M. CARTABIA, A. CELOTTO, *Introduzione,* in IID. (a cura di), *L'Europa dei diritti*, Bologna, Il Mulino, 2001, p. 14; M. CARTABIA, *Principi involabili e integrazione europea*, cit., pp. 37 ss.; D. BUTTURINI, *La tutela dei diritti fondamentali nell'ordinamento costituzionale italiano ed europeo*, cit., pp. 16 ss. e 40 ss.). Ricordando dunque come erano state affrontate le questioni relative alla protezione dei dati personali, prima in occasione dell'Accordo di Schengen e in seguito con la dir. 95/46, emerge chiaramente come, pur non trovando piena rispondenza nel diritto costituzionale degli Stati membri, la protezione dei dati personale avesse acquisito un ruolo di primo piano soprattutto all'interno dell'ordinamento costituzionale europeo. Tali impressioni, peraltro, trovano piena conferma anche nel rapporto elaborato dal Gruppo di esperti sui diritti fondamentali istituito dalla Commissione nel 1999 e presieduto da Spiros Simitis (già direttore del Centro di ricerca sulla protezione dei dati personali presso l'Università di Francoforte e garante per la protezione dei dati personali dello Stato dell'Assia; uno dei giuristi ad aver "inventato la protezione dei dati personali"). In quell'occasione, il Gruppo si era espresso constatando la sostanziale insufficienza del quadro normativo comunitario sulla protezione dei dati personali, mettendo in luce soprattutto le lacune relative alla regolamentazione delle materie riconducibili al secondo e al terzo pilastro. (Cfr. Commissione europea, *Per l'affermazione dei diritti fondamentali nell'Unione europea – Relazione del gruppo di esperti in materia di diritti fondamentali*, febbraio 1999, pp. 13 ss.)

[365] O. POLLICINO, M. BASSINI, *Articolo 8 – La protezione dei dati di carattere personale*, cit., pp. 134-135.

Innanzitutto, la possibilità di includere un diritto avente ad oggetto questo tema era stata attentamente vagliata alla luce dei quanto suggerito dal parere proposto dal Gruppo europeo per l'etica delle scienze e delle nuove tecnologie, un organo consultivo che fin da subito era stato attivamente coinvolto nei lavori preparatori della Carta[366].

Interpellati sul punto, poi, gli esperti del Gruppo Articolo 29 avevano manifestato un forte supporto alla possibilità di includere nel nuovo catalogo anche il diritto alla protezione dei dati personali, sottolineando come – seppur con modalità diverse – questo avesse già trovato conferma sia all'interno dell'ordinamento comunitario, sia in diversi contesti nazionali[367].

Infine, ad accogliere queste sollecitazioni, tra i membri dell'assemblea preposta alla redazione del testo della Carta, figurano studiosi storicamente legati al dibattito sulla protezione dei dati personali, tra cui il giurista francese Guy Braibant, il parlamentare spagnolo Jordi Solé Tura e l'accademico italiano Stefano Rodotà[368]; tutte sensibilità molto attente al tema in questione.

Alla luce di tutti questi elementi, dunque, si è cominciato a ragionare sull'opportunità di introdurre effettivamente una disposizione dedicata alla *sola* protezione dei dati, selezionando i contenuti da ricondurre a questo "nuovo" diritto fondamentale.

---

366 Nel mandato di presidenza italiana – guidata da Romano Prodi – la Commissione, infatti, aveva prontamente richiesto un parere proprio sull'opportunità di includere il diritto alla protezione dei dati personali nelle nuova Carta. Il Gruppo non solo aveva supportato tale ipotesi, ma con una preziosa opera di sintesi, aveva proposto una prima formulazione della norma, indentificando alcuni principi essenziali della materia (come la confidenzialità dei dati, il principio di finalità e il diritto di opposizione, i diritti di accesso, rettifica e cancellazione) nonché vietando l'utilizzo di tecnologie di sorveglianza troppo intrusive (Cfr. *Draft Chater of Fundamental Rights of the European Union,* CHARTE 4370/00 CONTRIB 233, Bruxelles, 15 giugno 2000, pp. 9 (con riferimento ai rischi legati alle nuove tecnologie dell'informazione) e 26 ss. (con i commenti del Gruppo consultivo)).

367 Gruppo Articolo 29, *Raccomandazione 4/99 concernente l'inclusione del diritto fondamentale alla protezione dei dati personali nella Carta europea dei diritti fondamentali* (WP26) 7 settembre 1999, pp. 3 ss.

368 G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection in the EU*, cit., p. 194.

La formulazione definitiva è quella che oggi si legge all'articolo 8 della Carta per cui

> 1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
> 2. 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. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.
> 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

La norma, evidentemente, fa propri una serie di principi già ampiamente riconosciuti dalla disciplina ordinaria, qui elevati però al rango di diritto fondamentale dell'UE.

La scelta di orientarsi verso una soluzione così creativa, come prevedibile, sul piano interpretativo ha sollevato non pochi problemi. La Carta, infatti, giusto all'articolo precedente, aveva comunque riconosciuto il diritto al rispetto della vita privata, stabilendo – in linea con l'art. 8 Cedu – che «ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni».

Comparando i contenuti degli artt. 7 e 8 CDFUE, si è trattato allora di capire in che rapporti sarebbero stati di lì in futuro i concetti di *privacy* e *data protection*, in quanto, pur avendosi formalmente due previsioni distinte, si era comunque di fronte a figure tra loro profondamente legate[369].

In ragion di ciò, soprattutto all'inizio, questa distinzione non ha trovato immediati riscontri. Certo si era ben consci del fatto che, con lo sviluppo delle tecnologie dell'informazione, la protezione dei dati personali avesse guadagnato nel tempo un ruolo di primo piano, tanto da rappresentare un logico compimento del diritto «ad essere lasciati soli». Allo stesso modo, però, si era altrettanto consapevoli che il sistema di garanzie legate ai dati fosse proiettato ben oltre la tutela della sola

[369] O. POLLICINO, M. BASSINI, *Articolo 8 – La protezione dei dati di carattere personale*, cit., pp. 134-135.

riservatezza delle informazioni, andando incontro invece ad una pluralità di valori e principi legati alla dimensione sociale della vita dell'individuo[370].

Su questo punto, vale la pena indugiare qualche istante.

Come già ricordato, la disciplina sulla protezione dei dati personali era nata con un obiettivo ben preciso, ossia quello di assicurare la tutela di una pluralità di interessi rispetto all'uso delle informazioni che riguardano una determinata persona. Per questo motivo, l'intera architettura normativa tradizionalmente gravita attorno a due concetti essenziali: quello di "trattamento" – richiamando tutti i sistemi attraverso cui i dati possono essere utilizzati – e, per l'appunto, quello di "dato personale".

Già ragionando sulla portata di quest'ultima nozione subito si colgono i problemi legati alla pretesa di una perfetta sovrapposizione tra *privacy* e *data protection*. Se infatti è abbastanza evidente che la tutela dell'autonomia privata non si esaurisce nella disciplina relativa ai flussi informativi, allo stesso modo sarebbe un errore ritenere che tutti i dati *personali* siano anche dati *riservati*[371].

In questa prospettiva si cominciano a cogliere le ulteriori estrinsecazioni del diritto alla protezione dei dati. Tale presidio, infatti, non ha come unica finalità

---

370 Nello specifico, rispetto al *quid pluris* della protezione dei dati personali rispetto alla *privacy*, si rimanda a M. TZANOU, *The Fundamental Right to Data Protection. Normative Value in the Context of Counter-Terrorism Surveillance*, Oxford-Portland (Oregon), Hart Publiching, 2017, pp. 21 ss.; L.A. BYGRAVE, *Data Protection Law: Approaching its Rationale Logic and Limits*, cit., pp. 133 ss; S. RODOTÀ, *Data Protection as a Fundamental Right*, in S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE, S. NOUWT (a cura di), *Reinventing Data Protection?,* New York, Springer, 2009, p. 45; S. GUTWIRTH, *Privacy and the Information Age*, cit., p. 79.

Rispetto alle possibili letture evolutive del concetto di *privacy,* invece, si vedano A. ROUVROY, Y. PULLET, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy?*, in S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE, S. NOUWT (a cura di), *Reinventing Data Protection?,* cit., p. 45; S. GUTWIRTH, *Privacy and the Information Age*, cit., p. 2.

371 Un punto sui cui la Corte di giustizia e il Tribunale di primo grado hanno avuto particolar modo di riflettere, soprattutto in occasione delle sentt. 8 novembre 2007, *The Bavarian Lager Co. Ltd c. Commissione delle Comunità europee* (T-194/04) §§ 118-119; 16 luglio 2015, *ClientEarth e Pesticide Action Network Europe (PAN Europe) c. Autorità europea per la sicurezza alimentare (EFSA)* (C-615/13), § 32.

quella di assicurare al singolo il *controllo* sulle informazioni che lo riguardano in chiave negativa. Esso si presta a promuovere una vera e propria *autonomia* informativa[372], definendo così nuovi punti di equilibrio tra una pluralità di interessi: dall'accesso agli atti, alla libertà di espressione, al diritto di difesa.

Il nuovo diritto sancito dall'art. 8 CDFUE, dunque, non solo «costituzionalizza» i principi cardine della disciplina, ma affranca definitivamente la protezione dei dati personali dalla logica economica con cui era stata concepita fino ad allora. L'introduzione di tale norma in una Carta dei diritti, infatti, contribuisce a mettere in risalto la funzione istituzionale di queste garanzie[373]; e questo non solo rispetto al valore della riservatezza ma soprattutto riguardo ai principi di dignità e di non discriminazione[374].

In un primo momento, però, le considerazioni appena esposte non sono risultate così immediate, incontrando anzi forti resistenze.

Sebbene il legislatore europeo negli atti approvati di lì in avanti non abbia mancato di ancorare le nuove normative sulla protezione dei dati personali a quanto previsto dalla Carta, questi riferimenti sono risultati spesso del tutto formali, quasi incapaci di valorizzare il *novum* sancito a Nizza. Come dimostrano infatti le direttive sull'*e-privacy* e sulla *data retention*, pur richiamando tale documento, l'obiettivo della regolamentazione conserva un approccio unitario in cui il trattamento delle

---

[372] O. POLLICINO, M. BASSINI, *Articolo 8 – La protezione dei dati di carattere personale*, cit., p. 136.

[373] Come evidenziato da diversi Autori, il percorso di "costituzionalizzazione" della protezione dei dati personali fatto nell'ordinamento europeo non solo ha emancipato queste garanzie dal diritto al rispetto della vita privata ma anche da un'interpretazione troppo individualistica. Il requisito del consenso – e così la logica tipica di un modello contrattuale – smette di essere al centro del sistema di tutele per lasciare più spazio al principio di legalità, e dunque al ruolo del legislatore e delle istituzioni statali e comunitarie, mirando alla realizzazione di «sistema di pesi e contrappesi» (O. POLLICINO, M. BASSINI, *Articolo 8 – La protezione dei dati di carattere personale*, cit., p. 136). Dello stesso avviso L.A. BYGRAVE, *Data Protection Law: Approaching its Rationale Logic and Limits*, cit., pp. ss.; L.A. BYGRAVE, D. SCHARTUM, *Consent, Proportionality and Collective Power*, in S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE, S. NOUWT (a cura di), *Reinventing Data Protection?,* cit. pp. 157, 162.

[374] M. TZANOU, *The Fundamental Right to Data Protection*, cit., pp. [28-31]; L.A. BYGRAVE, *Data Protection Law: Approaching its Rationale Logic and Limits*, cit., pp. ss.;

informazioni è letto soprattutto nell'ottica di salvaguardare la riservatezza dei contenuti[375]. Ed è per questo che normalmente l'art. 8 CDFUE compare spesso in pari con il precedente art. 7. Per molto tempo infatti il modello di riferimento ha continuato ad essere quello di Strasburgo, incentrato su un modello unitario fondato sull'art. 8 Cedu piuttosto che sul doppio binario proposto dalla Carta.

Quest'apparente confusione rispetto il distinguo operato dal legislatore, peraltro, trova piena conferma anche nella giurisprudenza di quegli anni, in cui tanto la Corte di giustizia quanto i suoi Avvocati generali dimostrano una sorta di disorientamento rispetto ai contenuti specifici della norma in esame.

Passando in rassegna le pronunce più significative, si coglie come inizialmente i giudici lussemburghesi avessero manifestato una certa indifferenza per il nuovo parametro introdotto dall'art. 8 CDFUE, continuando a leggere la protezione dei dati personali come una sottocategoria del diritto al rispetto della vita privata, secondo il modello consolidatosi attorno all'art. 8 Cedu[376].

Anche una volta superato questo primo ostacolo, i rapporti tra gli artt. 7 e 8 della Carta hanno continuano a rimanere comunque criptici. Nonostante la Corte UE osservi come il nuovo *bill of rights* assicuri specifiche tutele per i dati di carattere personale, da un punto di vista sostanziale, il punto cardine delle sue argomentazioni

---

[375] Il riferimento è alle direttive 2002/58 e 2006/24 (v. §§ 1.4 e 1.5) e in particolare, rispettivamente, ai *considerando* nn. 2 e 22, in cui si afferma come in entrambi i casi la disciplina miri a garantire il pieno rispetto dei diritti di cui agli articoli 7 e 8 della Carta, senza distinzione di sorta, quasi si trattasse di un'endiadi.

[376] Il riferimento più evidente, nonché il primo, è alla sentenza *Österreichischer Rundfunk e a.* in cui la Corte, rispetto ad una serie di ricorsi presentati tra il 2000 e il 2001 e decisi due anni più tardi, preferisce non fare alcuna menzione ai contenuti della Carta, rifacendosi invece, in tutto e per tutto, a quanto previsto dalla Cedu e dalla giurisprudenza di Strasburgo. Questa scelta è stata letta da alcuni con un processo di graduale transizione dal vecchio *sistema Strasburgo* al nuovo e autonomo *sistema Lussemburgo* (in generale M.E. GENNUSA, *La Cedu e l'Unione europea*, in M. CARTABIA (a cura di), *I diritti in azione*, cit., pp. 91 ss.; in particolare, G. GONZÁLEZ FUSTER, R. GELLERT, *The fundamental right of data protection in the European Unione: in serach of an uncharted right*, in *International Review of Law, Computers & Technology*, 26(1), p. 79). Altri, invece, hanno osservato come la stessa possa essere interpretata come una sostanziale indifferenza per i due sistemi di garanzie e per le loro reciproche differenze (O. LYNSKEY, *Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order*, cit., p. 575).

sembra rimanere il diritto al rispetto della vita privata. In diverse pronunce, infatti, quando si tratta di definire nuovi punti di equilibrio tra interessi contrapposti, normalmente i giudici europei sembrano far accedere al bilanciamento soltanto i valori relativi alla riservatezza, trascurando invece quelli legati all'autodeterminazione informativa in senso stretto. Nella sentenza *Promusicae*[377], ad esempio, la Corte, pur riconoscendo il distinguo tra l'art. 7 e l'art. 8 CDFUE, tende ad assimilare i due concetti ivi sanciti, leggendo quest'ultimo come un diritto volto a garantire «la tutela dei dati personali *e, quindi, [n.d.a.]* della vita privata»[378]. E così, nel bilanciamento tra valori contrapposti[379] verranno dunque in risalto soprattutto gli interessi legati alla sfera privata, piuttosto che non quelli relativa ad una vera e propria autodeterminazione informativa[380]. Analogamente, qualche anno più tardi, nella pronuncia *Satamedia*[381], i giudici lussemburghesi sembrano continuare ad evitare ogni riferimento, limitandosi a constatare come sia sufficiente rifarsi alla dir. 95/46[382] (nonostante i contenuti dell'art. 8 CDFUE avessero già trovato spazio nella giurisprudenza precedente).

In altri termini – come osservato nelle conclusioni sulla causa *Rijkeboer* – per lungo tempo l'impressione generale è stata quella di trovarsi ancora di fronte ad «un unico diritto, che [però ora] reca in seno un'intima contraddizione, poiché si sdoppia in due anime che lo trasformano in una specie di Dr. Jeckyl e Mr. Hyde»[383]. Tant'è

---

377 CGUE, sent. 29 gennaio 2008, *Productores de Música de España (Promusicae) contro Telefónica de España SAU* (causa C-275/06).

378 *Promusicae*, § 63.

379 Nel caso di specie la tutela della proprietà intellettuale e questa figura "ibrida", frutto dell'endiadi *privacy-data protection*.

380 *Ibidem*, § 65.

381 CGUE, sent. 26 dicembre 2008, *Tietosuojavaltuutettu contro Satakunnan Markkinapörssi Oy e Satamedia Oy* (causa C-73/07).

382 *Satamedia*, «La finalità di quest'ultima – si osserva – è che gli Stati membri, pur consentendo la libera circolazione dei dati personali, garantiscano la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, riguardo al trattamento di tali dati» (§ 52).

383 Conclusioni dell'AG D. Ruiz-Jarabo Colomer del 22 dicembre 2008, *College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer* (C-553/07), § 25.

che, nonostante alcuni prima cenni di apertura[384], prima del Trattato di Lisbona, in generale, le istituzioni europee hanno continuato a prediligere un approccio unitario, trascurando nelle loro interpretazioni la novità introdotta dall'art. 8 CDFUE.

In altri termini, dunque, il nuovo diritto alla protezione dei dati personali, a differenza di altri ben più consolidati, si era trovato oggetto di una sorta di «inversione cronologica»[385] tale per cui erano le fonti secondarie a legittimare una norma di (auspicato) ragno primario, ammettendo così una serie di incertezze circa l'effettiva portata del parametro.

### *3.3. La protezione dei dati personali come competenza dell'UE*

La situazione descritta poc'anzi sarebbe sensibilmente cambiata in seguito all'entrata in vigore del Trattato di Lisbona. Da un lato, infatti, a partire da quel momento, la Carta di Nizza – e così il diritto alla protezione dei dati personali *ex* art. 8 CDFUE – è diventata tutti gli effetti una fonte di rango primario, equiparata al diritto dei Trattati. Dall'altro, riprendendo quanto previsto dall'art. 286 TCE, l'art. 16 TFUE ha ulteriormente rafforzato la tutela di questo diritto, prevedendo alcune nuove competenze comunitarie.

Scorrendo il testo di quest'ultima norma si legge infatti che

> 1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
>
> 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale 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, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.

---

[384] Tribunale di primo grado, sent. 8 novembre 2007, *Commissione europea contro The Bavarian Lager Co. Ltd* (causa T-194/04) – poi impugnata dinnanzi alla CGUE e ribaltata con la sent. 29 giugno 2010 (Causa C-28/08 P).

[385]

> Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea.

Contestualizzando questa nuova disposizione nel quadro giuridico entro cui si colloca, va rilevato come gli accordi di Lisbona, in generale, abbiano contribuito a delineare una serie di caratteristiche che connotano l'identità europea, ancorandola ad una nuova tavola di valori[386].

Come si evince dal Preambolo, infatti, si tratta di un accordo caratterizzato da forte valenza culturale, valorizzando innanzitutto le «eredità culturali, religiose e umanistiche dell'Europa, da cui si sono sviluppati i valori universali dei diritti inviolabili e inalienabili della persona, della libertà, della democrazia, dell'uguaglianza e dello Stato di diritto»; un programma quindi teso a consolidare il progetto europeo, riassumendo nelle intenzioni gli obiettivi costituzionali già discussi qualche anno prima.

Questo cambio di prospettiva, per quanto riguarda la protezione dei dati personali, ha permesso di fare importanti passi in avanti, verso una più matura consapevolezza circa la funzione costituzionale di questo diritto.

Con il rapido sviluppo delle tecnologie digitali e con la rilevanza assunta dalla raccolta e dallo scambio di dati personali permessa dalla diffusione dell'Internet e

---

386 Un obiettivo che ormai ci si era prefissi da tempo, già a partire dai lavori per il Trattato di Nizza. In dottrina, *ex multis* si rimanda alle riflessioni di A. PIZZORUSSO, *Il patrimonio costituzionale europeo*, Bologna, Il Mulino, 2002; G.F. FERRARI, *I diritti tra costituzionalismi statali e discipline transnazionali*, in Id. (a cura di), *I diritti fondamentali dopo la Carta di Nizza*, cit., spec. pp. [5-7].

Quanto alla ricostruzione della storia e degli sviluppi istituzionali da Nizza a Lisbona, per al parte generale, ci si è rifatti soprattutto a R. BIN, P. CARETTI, G, PITRUZZELLA, *Profili costituzionali dell'Unione europea*, Bologna Il Mulino, 2015; P. COSTANZO, L. MEZZETTI, A. RUGGERI, *Lineamenti diritto costituzionale dell'Unione europea*, Torino, Giappichelli, 2014.

Quanto all'evoluzione storica e ai singoli passaggi, nello specifico, si rimanda, *ex multis,* a F. BASSINI, G. TIBERI (a cura di), *Una Costituzione per l'Europa. Dalla Convenzione europea alla Conferenza intergovernativa*, Bologna, Il Mulino, 2003 [spec. F. CLEMENTI, *La Convenzione sull'avvenire dell'Europa: il mandato, l'organizzazione, i lavori*, *ivi*; C. PINELLI, *Il preambolo, i valori, gli obiettivi*, *ivi;* F. PIZZETTI, *Le competenze dell'Unione*]; IID. (a cura di), *La Costituzione europea. Un primo commento*, Bologna, Il Mulino, 2004 []; Iid. (a cura di), *Le nuove istituzioni europee. Commento al Trattato di Lisbona*, Bologna, Il Mulino, 2008; J.H.H. WEILER, *La Costituzione dell'Europa*, cit.

dei servizi e delle piattaforme *online*, si è avvertita l'urgenza di introdurre una disposizione più incisiva di quanto in precedenza sancito dall'art. 286 TCE.

In particolare, i cambiamenti degli ultimi anni avevamo permesso di mettere a fuoco come la rivoluzione tecnologica in atto avrebbe avuto in futuro importanti ricadute sul mercato interno, fino a mettere in discussione il ruolo economico dell'Unione e delle sue imprese sul panorama internazionale[387]. L'avvento dei *new media* e dei *social network*, le proiezioni di sviluppo per il settore del *data brokering* e, soprattutto, le potenzialità economiche legate al mondo del *cloud,* dell'*internet of things* (IoT) e dell'intelligenza artificiale (Ai), cominciano ad aprire prospettive rispetto alle quali non si sarebbe potuti restare indietro. Allo stesso tempo, però, i progressi registrati in questi settori, non avevano fatto percepire soltanto le pressioni della concorrenza straniera, ma anche (e soprattutto) i rischi legati all'impatto di queste nuove tecnologie sui diritti individuali e gli equilibri istituzionali.

Alle questioni prettamente economiche, si erano quindi aggiunte delle ulteriori preoccupazioni, in parte inedite rispetto al passato, relative alle questioni di c.d. "sovranità digitale" e così alle implicazioni ultime dei nuovi regimi di sorveglianza istituiti dalle autorità pubbliche e dai sistemi di *intelligence* con il supporto degli operatori privati[388].

Alla luce di queste considerazioni, dunque, si è ritenuto opportuno rafforzare le prerogative dell'Unione in materia, non solo ribadendo la centralità del diritto alla protezione dei dati personali, ma riconoscendo anche una competenza di portata generale a livello europeo così da poter promuovere una più forte strategia di *data governance*.

---

387 H. HIJMANS, *The European Uninon as Guardian of Internet Privacy. The Story of the Article 16 TFEU*, cit.

388 A. SIMONCINI, *Sovranità e potere nell'era digitale*, in O. Pollicino, T.E. Frosini, E. Apa, M. Bassini (a cura di), *Diritti e libertà in Internet*, Milano, Mondadori, 2017, pp. 19 ss.; S. CALZOLAIO, *Protezione dei dati personali*, in *Digesto delle discipline pubblicistiche*, Torino, Utet, 2017 (edizione *online*), § I.2.

Analizzando puntualmente i contenuti della norma in esame, secondo quanto previsto dall'art. 16, § 1, TFUE, essa include il diritto alla protezione dei dati personali anche all'interno diritto dei Trattati, ammettendo così un regime diverso da quello previsto da quello previsto dalla sola Carta di Nizza, andando anche oltre le attività interne alle istituzioni europee e i compiti svolti dagli Stati membri in attuazione del diritto comunitario[389].

A ciò si aggiunge che, là dove la Carta aveva escluso la possibilità di estendere le competenze comunitarie[390], l'art. 16, § 2 riconosce esplicitamente delle nuove prerogative in capo al Parlamento europeo e al Consiglio UE, con un'unica eccezione per quanto riguarda le materie legate alla sicurezza nazionale[391]. L'articolo individua dunque una nuova materia nell'ambito della c.d. competenza concorrente[392].

Tuttavia, come osservato, sebbene tale norma conferisca alle istituzioni europee un forte discrezionalità in materia, per perseguire gli obiettivi di tutela indicati è necessario un solido coordinamento tra i diversi livelli di governo[393]. In concreto, infatti, il sistema di garanzie preposto alla protezione dei dati personali si sviluppa soprattutto a livello nazionale e presuppone che ciascuno Stato si faccia carico di tutte le iniziative necessarie a rendere effettivi i meccanismi di garanzia predisposti a livello europeo (dalla definizione della normativa di dettaglio, al corretto funzionamento delle autorità di controllo[394]) rendendo così i due sistemi profondamente interdipendenti.

---

389 Art. 51, § 1.

390 Art. 51, § 2.

391 Art. 39 TUE.

392 dal momento che la protezione dei dati comunque non compare all'interno dell'elenco *ex* art. 4 TFUE[392].

393 H. HIJMANS, *The European Uninon as Guardian of Internet Privacy. The Story of the Article 16 TFEU*, Svizzera, Springer International, 2016, pp. 128 ss.

394 Questo tratto era già evidente nel sistema promosso attraverso il prima pacchetto di misure sulla protezione dei dati personali, quello che gravitava attorno alla dir. 95/46. Fermo il fatto che trattandosi di una politica promossa attraverso un insieme di direttive, in questo caso, il

Questa nuova attribuzione di competenze, quindi, promette di avere forti conseguenze sul piano dei rapporti tra l'Unione e gli Stati membri.

Come ricordato, le attività che oggi implicano il trattamento dei dati personali – anche in processi molto complessi o comunque rischiosi per diversi diritti degli interessati[395] – coprono aree molto estese, intercettando ambiti e discipline assai diverse.

In astratto, dunque, risulta difficile capire fino a che o possano arrivare le norme disposte *ex* art. 16 TFUE e quelle che invece rimangono una prerogativa esclusiva del legislatore nazionale. E ciò risulta particolarmente evidente in alcuni contesti, in cui, per il tipo di diritti coinvolti, definire in modo chiaro il perimetro delle rispettive potestà risulta un'operazione critica; basti pensare ai problemi che già si incontrano nell'ambito delle politiche nazionali sulla sicurezza nazionale – materia rispetto al quale il richiamo all'art. 39 TUE sembra aver particolare riguardo – piuttosto che le questioni relativa alla libertà di espressione e informazione[396].

---

coinvolgimento del legislatore nazionale rappresentava un passaggio obbligato, in tutti i successivi sviluppi comunque non è mai venuto meno il ruolo cardine delle Autorità di controllo nazionale (art. 28 dir. 95/46). Va ricordato, ad ogni modo, come la Corte di giustizia, interpellata circa i requisiti a autonomia ed indipendenza di questi organi, negli anni successivi si sia pronunciata in più occasioni specificandone la natura e le funzioni, nonché gli obblighi imposti a livello nazionale ad un loro corretto funzionamento (CGUE, sentt. 9 marzo 2010, *Commissione europea c. Repubblica federale di Germania* (C-518/07); 16 ottobre 2012, *Commissione europea c. Repubblica d'Austria* (C-614/10); 8 aprile 2014, *Commissione europea c. Ungheria* (C-228/12)).

[395] Circa il tema del rischio in materia di protezione dei dati personali, in particolare, v. I. BÖRÖCZ, *Risk to the Right to Protection of Personal Data*, in *EDPL*, 4, 2016; R. GELLERT, *Understanding the notion of risk in the General Data Protection Regulation*, in *Computer Law and Security Review*, 2017; R. GELLERT, *Data Protection: a risk regulation? Between the risk management of everything and the precautionary alternative*, in *International Data privacy Law*, 5, 2015; N. VAN DIJK, R. GELLERT, K. ROMMETVEIT, *A Risk to a Right? Beyond Data Protection Impact Assessment*, in *Computer Law and Security Review*, 32, 2016.

[396] È già la stessa giurisprudenza comunitaria a documentare queste differenze. I giudici nazionali, infatti, nel rivolgersi alla Corte di giustizia, non solo tendono ad interpretare con sfumature diverse le definizioni e i concetti posti a fondamento della disciplina ma, dal modo in cui presentano le loro richieste di chiarimenti dimostrano di percepire in modi diversi le finalità stesse della disciplina. Se cioè per i Paesi dell'Europa orientale possono risultare cruciali le questioni legate ai limiti legali al trattamento dei dati personali, secondo una sensibilità orientata alla massima tutela della libertà personale, negli ordinamenti scandinavi i problemi emergono non tanto rispetto alla pubblicità di alcuni dati quanto rispetto alle possibilità di un loro riutilizzo per altri fini, in linea con

Alla luce di queste osservazioni, dunque, pur godendo di un'ampia competenza in materia, nell'ottica di promuovere gli elevati standard di tutele garantiti a livello comunitario, il legislatore UE, nell'esercitare le sue prerogative, è invitato a tenere in alta considerazione la portata del suo intervento e a coinvolgere ampiamente nelle sue decisioni anche i legislatori nazionali, favorendo un clima di leale collaborazione tra Bruxelles e gli Stati membri. In questo settore, infatti, vengono in luce questioni che chiedono un'attenta ponderazione tra gli interessi e gli obiettivi condivisi a livello europeo e le peculiarità dei singoli ordinamenti. Unitamente alle considerazioni relative all'osservanza dei principi di sussidiarietà e proporzionalità, dovranno così essere attentamente messi a fuoco i problemi legati al rispetto delle diverse identità nazionali – e questa volta, soprattutto, alle *diverse* tradizioni costituzionali.

### 4. Il regolamento 679/2016 e la nuova strategia di *data governance* europea

Come anticipato, il reg. 679/2016 rappresenta una disciplina di «ultima generazione»[397]. A distanza di vent'anni dall'approvazione della direttiva "madre", non solo si sono trasformate le tecnologie soltanto, ma è cambiata la realtà economica e sociale in cui esse vengono concepite e utilizzate. Analogamente, sono mutate le modalità con cui le informazione vengono prodotte e utilizzate, tanto da fare dei *big data* e delle applicazioni che da essi attingono una componente

---

la loro storica tradizionale di *open governement*. (Cfr. H. HIJMANS, *The European Uninon as Guardian of Internet Privacy. The Story of the Article 16 TFEU*, Svizzera, Springer International, 2016, pp. 128 ss.)

[397] V. MAYER-SCHÖNBERGER, *Generational Development of Data Protection in Europe*, in P.E. AGRE, M. ROTENBERG (a cura di), *Technology and Privacy: The New Landscape*, cit., p. 219.

infrastrutturale della vita associata, indispensabile sia nel settore pubblico che in quello privato[398].

Il regolamento, dunque, si cala in quest'ottica, aggiornando il quadro normativo con dei nuovi meccanismi di tutela pensati per le tecnologie *data intensive* [399] . Riprendendo l'approccio fondato sul principio di neutralità tecnologica[400], il documento in esame propone un insieme di prescrizione di carattere generale, individuando una serie di regole particolarmente duttili, così da adattarsi ai contesti più diversi: dai trattamenti di *dataset* di piccola entità, anche non automatizzati[401], fino alle attività più complesse e strutturate, come quelle svolte dai giganti tecnologici (i c.d. *over the top*) per i servizi proposti su scala internazionale[402].

---

[398] In tal senso, per descrivere la portata infrastrutturale dei dati, Luciano Floridi ha coniato il neologismo di *infosfera*, alludendo con quest'espressione la globalità dello spazio delle informazioni in tutti i diversi domini in cui queste possono essere prodotte e utilizzate (cfr. L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, Cortina Editore, 2017).

Analogamente, in termini di risorse informative, si è cominciato a guardare ai *big data* come il nuovo "oro nero" del Ventunesimo secolo. Lanciato provocatoriamente a mo' di *slogan* da Clive Humby (il primo ad aver pensato un sistema di fidelizzazione dei clienti attraverso l'utilizzo dei dati sugli acquisti delle carte fedeltà, nel 1994) *data is the new oil* è un assunto che negli ultimi anni ha offerto importati spunti di riflessione sul valore dei dati nell'economia contemporanea (Cfr. *The world's most valuable resource is no longer oil, but data. The data economy demands a new approach to antitrust rules*, in *The Economist*, 6 maggio 2017). Tale teoria, tuttavia, ha continuato e continua ad essere oggetto di discussione, soprattutto per l'ambiguità di un simile approccio al problema (B. MARR, *Here's Why Data Is Not The New Oil*, in *Forbes*, 5 maggio 2018).

[399] Il riferimento è rivolto soprattutto alla prescrizione di nuove misure di protezione *by design* e *by default* (art. 25), alle valutazioni di impatto sulla protezione dei dati personali (art. 35) e alla consultazione preventiva delle Autorità di controllo (art. 36) per i trattamenti che, interessando *dataset* particolarmente estensi o comunque ampie categorie di persone, rispetto ai quali il Regolamento prevede un dovere di controllo costante e l'obbligo di procedere in ottica preventiva. Per un'analisi più dettagliata di questi istituti, tuttavia, si rimanda agli approfondimenti proposti qui a seguito, al § 3.3.

[400] Reg. 679/2016, *considerando* n. 15 che, già dall'*incipit*, specifica come «al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate».

[401] Reg. 679/2016, art. 2, § 1: « Il presente regolamento 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».

[402] *Ibidem*, art. 3. Rispetto all'ambito di applicazione, soprattutto per le questioni emerse a seguito delle pronunce *Google Spain* e *Schrems* (cfr. G. FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in G. Resta, V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, Roma,

Per un'analisi dettagliata del testo normativo e per più puntuali commenti dei singoli istituti si rimanda all'ampia letteratura che in questi anni si è proficuamente cimentata sul tema[403]. Rispetto all'oggetto di questa ricerca, invece, per approfondire meglio il rapporto tra diritti fondamentali e *big data*, dopo una prima panoramica sulle novità introdotte dal regolamento, ci si soffermerà brevemente sulle evoluzioni delle strategie di *data governance* europea.

### *4.1. Il regolamento 679/2016: verso un nuovo modello unitario di tutela*

Nel 2009, anche sull'onda delle novità introdotte dal Trattato di Lisbona, con l'intento di promuovere una revisione sistematica del quadro complessivo della

---

Roma Tre-Press, 2015, pp. [121-128]) la norma prevede ampi margini per un'applicazione extra-territoriale della disciplina, disponendo, oltre al c.d. principio di stabilimento (art. 3, § 1, comunque ampliato rispetto a quanto stabilità dalla dir. 95/46, art. 4, § 1, lett. a) anche un nuovo principio c.d. di *target*, in ragione del quale il reg. 679/2016 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.» (art. 3, § 2).

[403] Tra i tanti, si rimanda a F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, voll. I-II, *Dalla Direttiva 95/46 al nuovo Regolamento europeo* e *Il Regolamento europeo 2016/679*, cit.; L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo : commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè, 2016; L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/ 679*, cit.; G. FINOCCHIARO (diretto da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017; F. DI RESTA, *La nuova privacy europea: i principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, Torino, Giappichelli, 2018; G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy,* Milano, Wolters Kluwer, 2018; C. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit.; R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato: commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice privacy): scritti in memoria di Stefano Rodotà*, Milano, Giuffrè, 2019.

normativa, la Commissione ha avviato un nuovo processo di riforma della disciplina sulla protezione dei dati[404].

Come già ricordato, si trattava di un'urgenza avvertita ormai da diversi anni. Guardando al quadro d'insieme, i principali riferimenti normativi erano rimasti quelli elaborati dalla Cedu e dalla Convenzione di Strasburgo del 1981, cui poi si erano aggiunti la dir. 95/46, il reg. 2001/45, la dir. 2002/58 e la dir. 2006/24. Il sistema di tutele risultava quindi evidentemente datato, pensato per una società che, pur conoscendo Internet e i trattamenti automatizzati, si concentrava soprattutto su archivi e banche dati chiuse, guardando ad una realtà ben lontana dalla rivoluzione del *web 2.0* e del *digital by default*[405].

Per una serie di motivi, tuttavia, per molto tempo si era stati particolarmente cauti nel rimettere mano ai contenuti della direttiva "madre". Da un lato, infatti, con l'allargamento dell'Unione, si era preferito procrastinare ogni intervento radicale, così da permettere agli Stati candidati di adeguare i propri ordinamenti ai complessi requisiti previsti dall'*acquis* di Schengen[406]. Dall'altro, poi, viste le tensioni legate al terrorismo internazionale, si erano registrate particolari ritrosie rispetto ad una possibile riforma della disciplina sulla protezione dei dati in termini più garantistici,

---

[404] Commissione europea, *Comunicazione della Commissione al Parlamento Europeo e al Consiglio - Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini* (COM (2009) 262), 6 giugno 2009, pp. 8-9.

[405] Si cominciava a discutere, all'epoca, del piano d'azione della Commissione per l'attuazione del programma di Stoccolma (COM(2010) 171 def.) dell'Agenda digitale europea (COM(2010) 245 def.) e, più in generale, della strategia Europa 2020 dell'UE (COM(2010) 2020 def.).

[406] Dal 1997 al 2009, infatti, l'Unione era passata da quindici a ventotto Stati, di cui molti – soprattutto i Paesi dell'Europa orientale – portavano con sé storie e culture profondamente diverse e discontinue rispetto a quelle dei Paesi fondatori (cfr. L. CALIFANO, *Il Regolamento UE e la costruzione di un modello uniforme di diritti europeo alla riservatezza e alla protezione dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/ 679*, cit., p. 17). Se alcuni hanno visto in queste vicende un iniziale motivo di rallentamento alla riforma della disciplina (cfr. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, vol. I, *Dalla Direttiva 95/46 al nuovo Regolamento europeo*, cit. p. 37), in seguito, altri hanno visto in questo nuovo assetto allargato una delle ragioni principali per passare da una direttiva ad un regolamento, a fronte dell'urgenza di una disciplina ad effetto diretto (cfr. L. CALIFANO, *Il Regolamento UE,* cit.; L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, cit., p. 70).

tanto da aver escluso un intervento nell'ambito delle competenze afferenti al terzo pilastro preferendo orientarsi verso delle misure di armonizzazione[407].

Allo stesso tempo, però, considerando anche i fattori di segno opposto, i limiti della normativa vigente si erano resi quanto mai evidenti. La diffusione dei servizi in rete, infatti, aveva reso lo scambio internazionale di dati da uno Stato all'altro una prassi ormai del tutto normale, e questo non solo all'interno dell'area europea ma anche verso i Paesi terzi. A ciò poi si andavano aggiungendo le novità legate agli ultimi sviluppi delle tecnologie *data-intensive*, con la messa a punto di programmi e applicazioni sempre più sofisticati e complessi.

La consultazione avviata nel luglio 2009 ha offerto dunque una prima occasione per affrontare in modo sistematico i problemi appena accennati.

Il Gruppo Articolo 29 e il Gruppo di lavoro Polizia e Giustizia, in un parere congiunto dal emblematico titolo *The future of privacy*[408], avevano messo in luce, come nell'insieme, i capisaldi dalla direttiva "madre"[409] rappresentassero ancora dei validi presupposti per far fronte ai rischi legati alla globalizzazione e all'automazione dei trattamenti[410]. Tuttavia, analizzando la disciplina nel suo complesso se, per un verso, da un punto di vista prettamente normativo, si percepiva l'urgenza di adottare nuovi standard di protezione a livello global[411]; dall'altro, guardando al dato tecnologico, si

---

[407] Dir. 2006/24.

[408] Gruppo Articolo 29, Gruppo di lavoro "Polizia e Giustizia", *The Future of Privacy – Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data* (WP 168) del 1 dicembre 2009.

[409] *Ibidem*, § come, ad esempio, i principi di legalità, correttezza e trasparenza; il principio di finalità; la qualità dei dati –

[410] *Ibidem*, § 42.

[411] Proprio in quegli anni si è osservato come non solo fosse auspicabile raggiungere degli standard globali sulla protezione dei dati personali (un risultato cui né ora né allora si è stati in grado di raggiungere) ma come fosse desiderabile raggiungere dei punti di chiarimento anche sui presupposti di applicazione della disciplina comunitaria, sia rispetto ai criteri per l'individuazione della legge applicabile (WP29, WPPJ, *The Future of privacy*, cit., § 29). Sul fronte interno, il Gruppo Articolo 29 si era prodigato, in particolare, con alcuni pareri volti a chiarire il significato delle definizioni di base, come, ad esempio, le nozioni di dato personale, di responsabile del trattamento e di consenso. Più in generale, verso l'esterno, durante la Conferenza internazionale delle Autorità garanti per la protezione dei dati personali del 5 novembre 2009, si era cominciato a lavorare a degli

avvertiva l'esigenza di introdurre nuove misure al passo con l'innovazione, soprattutto nell'ottica di incentivare la tutela *by design*[412].

Tali urgenze, in particolare, si erano rese palesi soprattutto nei numerosi pareri con cui il Gruppo Articolo 29 è intervenuto per far fronte ai problemi che emersi nei diversi settori, adattando di volta in volta le previsioni originarie alle esigenze del nuovo contesto. Le questioni spaziano dalla protezione dei dati personali nell'utilizzo dei motori di ricerca e nella gestione dei *social network*, all'utilizzo di contatori intelligenti, dalla geo-localizzazione dei dispositivi mobili ai c.d. "confini intelligenti", fino ad arrivare alla pubblicità comportamentale, ai *big data*, all'*internet of things*[413].

Si tratta di un elenco che, per come documenta le molteplici e poliedriche evoluzioni delle tecnologie *data intensive,* in qualche modo parla da solo. Analizzando, infatti, in chiave trasversale il contenuto dei diversi pareri, si coglie il tentativo volto a favorire un'interpretazione organica e coerente della disciplina nonostante il

---

standard internazionali da promuovere negli anni a venire anche rispetto alle relazioni internazionali degli Stati membri e dell'Unione (obiettivo subito messo a tema nel Programma di lavoro 2010-2011 (WP170), p. 3, § II).

412 WP29, WPPJ, *The Future of privacy*, cit., §§ 29. Nel parere, tuttavia, non si manca di levare come già la dir. 95/46 in diversi passaggi prevedesse degli accenni alla protezione *by design*, pretendendo l'adozione di adeguate misure tecniche e organizzative (rimandando, in particolare, agli artt. 6, 16, 17 e al considerando n. 46; cfr. § 44). L'invito, tuttavia, è quello di addivenire ad una previsione più puntuale, in grado di chiarire in modo sistematico i presupposti e i requisiti di questo tipo di misure (§§ 45 ss.)

413 Gruppo Articolo 29, parere del 4 aprile 2008, *Opinion 1/2008 on data protection issues related to search engines* (WP138); parere del 12 giugno 2009, *Opinion 5/2009 on online social networking* (WP163); parere del 22 giugno 2010, *Opinion 2/2010 on online behavioral advertising* (WP171); parere del 6 maggio 2011, *Opinion 13/2011 on Geolocation services on smart mobile devices* (WP185); parere del 22 marzo 2012, *Opinion 02/2012 on facial recognition in online and mobile services* (WP192); parere del 27 aprile 2012, *Opinion 3/2012 on developments in biometric technologies* (WP193), parere 1 luglio 2012, *Opinion 05/2012 on Cloud Computing* (WP196); parere del 27 febbraio 2013, *Opinion 02/2013 on apps on smart devices* (WP202); parere 6 giugno 2013, *Opinion 05/2013 on Smart Borders* (WP206); parere del 4 dicembre 2013, *Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force* (WP209); parere 16 settembre 2014, *Opinion 8/2014 on the on Recent Developments on the Internet of Things* (WP223).

progresso tecnologico, adattando concetti, diritti e obblighi pensati per una realtà *small data* attraverso queste fonti di *soft law*.

Con l'andar del tempo, dunque, proprio alla luce dei suggerimenti già proposti nel 2009[414], la Commissione ha quindi deciso di promuovere una revisione sistematica della normativa in materia, presentando, nel 2012, la proposta di un regolamento generale[415] che sarebbe diventata la nuova «pietra angolare»[416] dell'architettura normativa[417]. Consapevoli dell'arretratezza della normativa vigente e degli elevati standard di tutela pretesi a livello europeo dalla Carta di Nizza e dal TFUE[418], si avvertiva infatti la definitiva l'urgenza di cambiamento; una riforma in grado di dare sistematicità e forza vincolante alle indicazioni fino ad allora promosse soltanto attraverso le fonti di *soft law*.

---

[414] WP29, WPPJ, *The Future of Privacy*, cit.

[415] Commissione europea, *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.), 25 gennaio 2012.

[416] Così la Commissione aveva definito la sostituenda direttiva 95/46, introducendo la proposta del nuovo regolamento generale sulla protezione dei dati personali (COM (2012)11 def., p. 1).

[417] In particolare, nell'ottica promossa nel 2009, ci si aspettava l'intervento sarebbe stato poi promosso soprattutto nell'ambito della disciplina relativa alle attività riconducibili a quello che fin prima del Trattato di Lisbona era stato il c.d. terzo pilatro (cooperazione giudiziaria e di polizia in materia penale); il settore che, alla luce di quanto previsto dall'art. 8 CDFUE e dall'art. 16 TFUE, risultava maggiormente critico. (cfr. WP29, WPPJ, *The Future of Privacy*, cit., § 5). Sulla base di tali considerazioni, come si vedrà meglio a breve in questo paragrafo, si comincerà a lavorare dapprima ad un progetto di direttiva generale per la protezione dei dati personali nell'ambito della sicurezza pubblica della giustizia penale (quella che oggi è la dir. UE 680/2016) e, in seguito, ad una direttiva specifica circa l'utilizzo dei codici PNR (dir. UE 682/2016). In dottrina, a commento di queste evoluzioni, si rimanda a P. MILAZZO, *La Direttiva UE 2016/680 e la protezione dei dati personali nell'ambito della sicurezza pubblica e della giustizia penale*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/ 679*, cit., pp. 709 ss.

[418] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni – Salvaguardare la privacy in un mondo interconnesso. Un quadro europeo della protezione dei dati per il XXI secolo* (COM (2012) 9 def.), 25 gennaio 2012.

*a. Il passaggio da una direttiva a un regolamento*

Ripercorrendo il lungo *iter* che ha portato all'approvazione del reg. 679/2016, il primo elemento meritevole di attenzione riguarda proprio la scelta di uno strumento *self executing*, passando da una direttiva a un regolamento.

A fronte dell'allargamento dell'Unione e dei crescenti scambi di informazioni a livello transfrontaliero e internazionale, infatti, si era giunti a concludere fosse ormai necessario orientarsi verso un nuovo modello, in grado di definire un unico regime normativo su tutto il territorio europeo (*one continent, one law*)[419].

Chiaramente, il rafforzamento delle basi giuridiche ha giocato un ruolo fondamentale in questa scelta. Il fatto, nel diritto europeo, che la protezione dei dati personali costituisca un diritto fondamentale di primo piano[420] e che l'Unione goda di una competenza particolarmente estesa[421] in quest'ambito, ha permesso di rafforzare il sistema di tutele in quella prospettiva di più ampio respiro cui tanto si era auspicato[422], così superando definitivamente la prospettiva *market-oriented* che aveva guidato il legislatore nell'approvazione della direttiva "madre"[423].

---

[419] Come ricordato in L. Califano, *Privacy: affermazione e pratica di un diritto fondamentale*, cit., p. 70, fu questo il motto promosso dal Vicepresidente della Commissione, Vivian Reding, nella prospettiva di incoraggiare non solo l'adozione di un disciplina comune all'interno dell'Unione ma anche la creazione di un vero e proprio *global standard* (cui poi era stata dedicata la Dichiarazione di Madrid del 2009).

[420] Il riferimento, come intuibile, è a quanto previsto dall'art. 8 CDFUE e dall'art. 16, § 1 TFUE.

[421] Art. 16, § 2, TFUE.

[422] COM (2012) 11 def., § 3.1, in cui, oltre alle norme appena ricordate nelle note precedenti, si richiama inoltre l'art. 114, § 1, TFUE, per quanto «necessario soltanto in relazione alle modifiche della direttiva 2002/58/CE in quanto la direttiva prevede anche la tutela dei legittimi interessi degli abbonati che sono persone giuridiche» (ora oggetto anch'essa di revisione: COM (2017) 10 def.).

[423] La quale, come ricordato, era ancorata a quanto previsto dall'art. 100A TCE, nell'ambito delle misure volte a promuovere il mercato unico e la libera circolazione.

In ossequio ai principi di sussidiarietà e proporzionalità, tuttavia, simili presupposti, di per sé, non sarebbero bastati per determinarsi verso l'opzione del regolamento[424], richiedendo quest'ultima un'analisi ben più rigorosa.

In tal senso, in primo luogo, si è messo subito in luce come l'art. 8 CDFUE, sancendo un diritto fondamentale, pretende che venga assicurato lo stesso livello di tutela in tutto il territorio dell'Unione; un obiettivo cui la direttiva "madre" aveva evidentemente faticato a tener fede[425].

In secondo luogo, guardando allo *status quo*, si è evidenziato come le varie normative di recepimento già mostrassero sensibili differenze, tanto che ipotizzando una nuova direttiva si intravedeva in concreto il rischio di consolidare «livelli diversi di protezione negli Stati membri e di creare restrizioni nei flussi transfrontalieri di dati personali tra gli Stati membri dotati di norme differenti»[426].

Infine, si è osservato come sempre più spesso le attività di trattamento riguardino l'utilizzo di servizi in rete, favorendo così un crescente scambio di dati a livello internazionale; una situazione che avrebbe messo l'Unione in una posizione privilegiata nell'assicurare elevati livelli di tutela, là dove gli Stati membri non riescono ad arrivare[427].

---

[424] Dal momento che, come accennato, quella prevista dall'art. 16, § 2, TFUE non costituisce una competenza esclusiva, bensì una competenza concorrente, il legislatore europeo nell'esercizio delle sue prerogative è tenuto a valutare l'adeguatezza delle proprie iniziative rispetto ad entrambi, secondo quanto previsto dall'art. 5, § 3 TUE e dal protocollo n. 2 sull'applicazione dei principi di sussidiarietà e di proporzionalità.

[425] COM (2012) 11 def., § 3.2, osservazioni ereditate dal regolamento stesso in cui, nell'ambito dei *considerando,* si legge che «sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche...» (n. 9) e pertanto: « Per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici» (n. 13).

[426] *Ibidem.*

[427] *Ibidem,* § 3.2, punti 3 e 4, in cui si legge che mentre «[L']Unione si trova nella posizione migliore per garantire in maniera efficace e coerente lo stesso livello di protezione alle persone

Alla luce di queste considerazioni, dunque, ferma la possibilità di completare la normativa europea a livello nazionale – anche innalzandone gli standard di tutela – si è guardato con favore alla possibilità di intervenire con un regolamento, soprattutto nell'ottica di promuovere un modello più centrale. Eccezion fatta per alcune materie particolarmente sensibili – come, ad esempio, la legislazione in ambito penale, giuslavoristico, amministrativo – la nuova disciplina, dunque, delineando un impianto dalla *ratio* unitaria, sancisce i principi e le prescrizioni generali dell'intera materia, individuando un insieme di norme alle quali ogni altra disciplina specifica è tenuta a rifarsi.

*b. Le peculiarità della tecnica normativa*

Confrontando la nuova normativa con la precedente, le differenze, quanto meno in termini quantitativi risultato evidenti. Il regolamento, strutturato in sei distinti capi, conta novantanove articoli accompagnati da più di centosettanta *considerando*, in sostituzione di una direttiva che – ormai vent'anni prima – ne conteneva circa un terzo.

Addentrandosi in questo nuovo enorme «edificio di nozioni, regole e precetti»[428], oltre a notare la fitta trama di disposizioni con cui l'interprete è chiamato a cimentarsi, è interessante notare come la tecnica normativa si sia evoluta nel tempo.

Aumentati di numero, i *considerando* guadagnano infatti un ruolo di primo piano. Da una lista di indicazioni orientative si passa ad una serie di valutazioni complesse, ricche di contenuti e volta a mettere in luce non solo le ragioni storiche

---

fisiche i cui dati personali siano trasferiti verso paesi terzi», «gli Stati membri non sono in grado da soli di risolvere i problemi posti dalla situazione attuale, in particolare dalla frammentazione delle legislazioni nazionali».

[428] V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 10.

che hanno portata alla riforma della disciplina, ma anche le preoccupazioni emerse nel corso della discussione, nonché i criteri che, in prospettiva, dovranno guidare la corretta interpretazione delle singole prescrizioni. Si documenta, in altre parole, la mutata *ratio* della disciplina: la «funzione sociale della protezione dei dati personali»[429] come diritto fondamentale e i rapporti che intercorrono tra questa nuova figura e quelle di più storico lignaggio[430], in linea con l'inevitabile pervasività cui si prestano le tecnologie *data-intensive*.

Questa maggior consapevolezza rispetto al ruolo della disciplina sui dati nel contesto odierno emerge peraltro anche nella formulazione delle diverse norme, evidentemente orientate al bilanciamento tra interessi contrapposti. Come si evince dalla prima disposizione, infatti, nonostante la centralità dell'approccio *rights-oriented*, il regolamento continua a porsi nell'ottica di perseguire due diversi obiettivi: da un lato, la tutela dei «diritti e le libertà fondamentali delle persone fisiche, [e] in particolare il diritto alla protezione dei dati personali»; dall'altro, la libera circolazione dei dati[431].

Analizzando la tecnica normativa, dunque, si osserva come forti enunciazioni di principio siano normalmente accompagnate ad una serie di eccezioni e deroghe, volte a rendere flessibili i contenuti prescrittivi in funzione delle caratteristiche dei diversi contesti (finanche a riplasmare caso per caso l'originaria portata delle singole disposizioni)[432].

---

[429] Reg. 679/2016, *considerando* n. 4.

[430] *Ibidem*, in cui si legge, peraltro, come l'attenzione del legislatore europeo, alla luce di quanto previsto dalla Carta, si sia concentrata non solo sul rispetto della vita privata (art. 7 CDFUE) ma su *tutti* i diritti sanciti dalla Convenzione di Nizza (cfr. « Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai 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»).

[431] Reg. 679/2016, art. 1.

[432] V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 16.

Come già ricordato, chiaramente, il reg. 679/2016, pur proponendo un modello unitario, ammette comunque alcuni margini di intervento in capo al legislatore nazionale, chiamato ora ad integrare e dare attuazione a quanto previsto dalla disciplina, ora a prevedere – a sua discrezione – più elevati standard di tutela in alcuni specifici settori[433].

*c. I principi generali e il concetto di dato personale*

Alla luce delle considerazioni esposte poc'anzi, vale la pena soffermarsi brevemente su alcuni principi generali della disciplina, evidenziando le novità introdotte dalla riforma.

Quanto all'ambito di applicazione materiale, rientrano nel perimetro del regolamento *tutti* i trattamenti di dati personali – interamente o parzialmente automatizzati, o non automatizzati affatto – purché volti alla creazione di un archivio[434]. Fanno eccezione a questa regola generale soltanto le materia non espressamente attribuite all'Unione o disciplinate da altre fonti[435], così come

[433] Reg. 679/2016, Capo IX.

[434] Reg. 679/2016, art. 2, § 1 e *considerando* n. 15 (secondo e terzo periodo).

[435] *Ibidem*, art. 2, § 2, secondo le quali sono esclusi i trattamenti di dati personali «effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione» (lett. a); «effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE» (lett. b) ossia quelli inerenti la c.d. *azione esterna* soprattutto in materia di politica estera e sicurezza comune e, infine, quelli « 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» (lett. d) ai quali in parte si applicano le disposizioni introdotte dalla dir. 680/2016. In dottrina, A. SPANGARO *L'ambito di riferimento materiale del nuovo Regolamento*, in G. FINOCCHIARO (diretto da) *Il nuovo Regolamento europeo sulla privacy*, cit., pp. 29-30; C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., pp. 95 ss.

l'utilizzo dei dati ad opera dalle persone fisiche «per l'esercizio di attività a carattere esclusivamente personale e domestico» (c.d. *household exclusion provision*)[436].

Quanto invece all'ambito di applicazione territoriale, alla luce delle criticità emerse nell'affrontare le questioni legate alla protezione dei cittadini europei rispetto ai trattamenti dei loro dati operati da soggetti estranei alla giurisdizione comunitaria[437], il regolamento introduce importanti novità. Accanto allo storico criterio dello stabilimento (anch'esso ampliato e rivisto[438]) è stato aggiunto infatti il c.d. principio del *targeting*[439], tale per cui per le attività che riguardino l'offerta di beni,

---

[436] Reg. 679/2016, art. 2, § 2, lett. c. Un principio, quello dell' *household exclusion provision*, già presente nella dir. 95/46 (art. 3, § 2, secondo periodo) ma che con lo sviluppo dei *social network* e degli altri servizi offerti dalle piattaforme *online* acquista un ruolo e un significato critico. Come dimostrato all'epoca dalla decisione sul caso *Lindqvist*, pur essendoci oggi dei criteri cui ispirarsi per distinguere tra un trattamento professionale-commerciale e uno personale-domestico (A. SPANGARO *L'ambito di riferimento materiale del nuovo Regolamento*, cit., p. 35), la linea di confine è destinata ad essere sempre meno netta (basti pensare all'utilizzo di quei servizi in cui le due dimensioni risultano già sovrapposte come *Linkedin* e *Facebook*). Per una più ampia trattazione del tema si rinvia in particolare a B. VAN ALSENOY*, Data Protection Law in the EU: Roles, Responsibility and Liability*, Anversa, Intersentia, 2019, pp. .

[437] Il riferimento va a quanto già accennato con riferimento ai casi *Google Spain* e *Schrems* (e in termini analoghi, seppur diversi, )

[438] Comparando infatti quanto disposto dall'art. 4, § 1, dir. 95/46, sul diritto nazionale applicabile si legge che: «Ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali: a) effettuato *nel contesto delle attività di uno stabilimento* del responsabile del trattamento *nel territorio dello Stato membro* […]; b) *il cui responsabile non è stabilito nel territorio dello Stato membro*, ma in un luogo in cui si applica la sua legislazione nazionale, a norma del diritto internazionale pubblico; c) il cui responsabile, non stabilito nel territorio della Comunità, ricorre, ai fini del trattamento di dati personali, *a strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro*, a meno che questi non siano utilizzati ai soli fini di transito nel territorio della Comunità europea…». Il reg. 679/2016, invece, all'art. 3, §§ 2-3, quanto all'ambito di applicazione territoriale aggiunge che: «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. 3. Il presente regolamento si applica 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.»

[439] L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*,

la prestazione di servizi o il monitoraggio del comportamento degli interessati all'interno dello spazio geopolitico europeo, troverà comunque applicazione la nuova disciplina, anche quanto lo stabilimento del titolare si trovi al di fuori del territorio dell'Unione.

Ciò premesso, quanto ai concetti chiave della normativa, particolare attenzione meritano le innovazioni intervenute nell'impianto definitorio. Per assicurare un elevato livello di tutela e la possibilità di dare amplia applicazione alla nuova disciplina, il reg. 679/2016, oltre ad introdurre *ex novo* diverse nozioni[440] (vedi, ad esempio, quella di «consenso»[441]) rafforza e amplia la portata dei concetti di base includendo «qualsiasi informazione riguardante una persona fisica identificata o identificabile»[442] e specificando una serie di elementi che normalmente rientrano in tale categoria (così recependo gli orientamenti maturati negli anni nei pareri del Gruppo Articolo 29[443]). Si considerando infatti dati personali non solo le

[440] Scorrendo l'art. 4, reg. 679/2016, si pensi, ad esempio, al concetto di «limitazione del trattamento» (n. 3); «profilazione» (n. 4); «pseudonimizzazione» (n. 5); «consenso dell'interessato» (n. 11); «violazione dei dati personali» (n. 12); «dati genetici» (n. 13); «dati biometrici» (n. 14); «dati relativi alla salute (n. 15); «stabilimento principale» (n. 16); «rappresentante» (n. 17); «impresa» (n. 18); «gruppo imprenditoriale» (n. 19); «norme vincolanti d'impresa» (n. 20); «autorità di controllo» (n. 21); «autorità di controllo interessata» (n. 22); «trattamento transfrontaliero» (n. 23); «obiezione pertinente e motivata» (n. 24); «servizio della società dell'informazione» (n. 25); «organizzazione internazionale» (n. 26).

[441] Nonostante la centralità del concetto, infatti, in precedenza non era stata elaborata alcuna definizione specifica nell'ambito della normativa europea. Ora invece è inteso come: «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento» (reg. 679/2016, art. 4, n. 11).

[442] Reg. 679/2016, art. 4, n. 1.

[443] Leggendo la seconda parte della definizione proposta dall'art. 4, n. 1, si legge infatti che possono essere rientrare nel concetto di dato personale diverse tipologie di informazione, «con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale». A questi si aggiungono poi concetti specifici come quelli di «pseudonimizzazione», «dato biometrico» e «dato genetico»; tutta una serie di nozioni già oggetto di riflessione soprattutto nel parere del 6 maggio 2011, *Opinion 13/2011 on Geolocation services on smart mobile devices* (WP185); parere del 22 marzo 2012, *Opinion 02/2012 on facial recognition in online and mobile services* (WP192); parere del 27 aprile 2012, *Opinion 3/2012 on developments in biometric technologies* (WP193).

informazioni immediatamente identificative, bensì anche i contenuti che possono contribuire ad individuare l'interessato anche solo indirettamente, lasciando così esclusi dall'ambito di applicazione soltanto i dati anonimi, valutando *tutti* i mezzi di cui ci si potrebbe avvalersi ai fini della re-identificazione e «tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici»[444].

*d. Le garanzie a tutela dell'interessato*

Sempre con lo scopo di incentivare un elevato livello di tutela dei dati, per quanto riguarda la disciplina sostanziale, il legislatore europeo è intervenuto in due direzioni, da un lato, potenziando il sistema dei diritti e delle garanzie a favore dell'interessato e, dall'altro, innovando il quadro degli obblighi e dei doveri in capo al titolare del trattamento.

Quanto al primo di questi due profili, al centro dell'architettura normativa si conferma il principio di trasparenza; un caposaldo volto a ribilanciare le asimmetrie informative e operative che normalmente caratterizzano la posizione dell'interessato nei confronti del titolare.

Innanzitutto, il regolamento definisce in modo dettagliato i requisiti del consenso e dell'informativa, ampliando notevolmente la portata di questi istituti. Oltre ad individuare nell'accettazione uno delle principali condizioni di liceità del trattamento[445], il regolamento prevede che di norma la dichiarazione debba essere espressa e sostanziarsi in un atto positivo ed inequivocabile[446]. Si ammette inoltre la

---

[444] Reg. 679/2016, *considerando* n. 26.

[445] Reg. 679/2016, art. 6.

[446] Il riferimento puntuale è all'art. 7, che prevede innanzitutto che il titolare del trattamento sia in grado «di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali» (§ 1). Dispone poi che, nel caso in cui la prestazione del consenso sia richiesta nel contesto di una dichiarazione scritta unitamente ad altre materie, questa sia « presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro» (§ 2); condizione di particolare importanza se si

possibilità che la stessa possa essere revocata in ogni momento con la stessa facilità con cui è stata originariamente prestata[447], prevedendo alcuni requisiti speciali quanto si trattino particolari categorie di dati[448] e quando il trattamento coinvolga soggetti minori d'età[449].

Quanto all'informativa[450], sempre in ossequio il principio di trasparenza, è stabilito che il soggetto sia messo nelle condizioni di conoscere l'identità del titolare, così come le caratteristiche, la logica e le finalità del trattamento[451]. Considerata la complessità delle attività svolte, i riferimenti devono essere proposti sempre in «forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro», anche ricorrendo all'utilizzo di illustrazioni o icone. L'interessato deve essere informato sulla fonte da cui provengono i dati utilizzati qualora non li abbia forniti egli stesso[452] e, in ogni caso, devono sempre essergli fornite le informazioni necessarie all'esercizio dei suoi diritti.

In merito a quest'ultimo punto, alla luce della particolare attenzione prestata in generale a questo tema, il GDPR ha contribuito a rinnovare profondamente il quadro delle garanzie riconosciute a favore dell'interessato, ampliando sensibilmente il suo *bill of rights* in materia di dati personali.

Unitamente ad alcuni diritti riconosciuti anche dalla direttiva – come, ad esempio, il diritto di accesso[453], il diritto di rettifica e di integrazione[454] o il diritto di

---

considera che molto spesso la richiesta di accettazione è posta in calce alle condizioni generali di contratto o presentata contestualmente ad altre richieste di accettazione (ad esempio in ambito medico, unitamente all'accettazione del trattamento sanitario). F. BRAVO, *Il consenso e le altre condizioni di liceità*, in G. FINOCCHIARO (diretto da), *Il nuovo Regolamento europeo sulla privacy*, cit., pp. 158;

[447] Reg. 679/2016, art. 7, § 3.
[448] *Ibidem*, artt. 9 e 10.
[449] *Ibidem*, art. 8.
[450] *Ibidem*, art. 12.
[451] *Ibidem,* art. 13
[452] *Ibidem,* art. 14.
[453] *Ibidem,* art. 15.
[454] *Ibidem*, art. 16.

limitazione di trattamento[455] – il regolamento ha introdotto alcune nuove figure di particolare interesse, soprattutto rispetto alla realtà delle tecnologie *data-intensive*.

In primo luogo, merita attenzione il diritto alla cancellazione, noto anche come «diritto all'*oblio*». Nonostante la giurisprudenza nazionale[456] ed europea[457] avessero già avuto ampio modo di cimentarsi anche con alcune pronunce "anticipatorie", è solo con la nuova disciplina che questo «diritto senza legge»[458] ha infatti acquisito una sua autonoma dignità[459].

Per prima cosa, questa figura non è più circoscritta alla sola deindicizzazione dei risultati proposti dai motori di ricerca ma, in generale, identifica una pretesa volta alla cancellazione dei dati senza ingiustificato ritardo. Onde evitare interpretazioni espansive del diritto in questione, il legislatore ha poi previsto una

---

[455] *Ibidem*, art. 18.

[456] La Corte di cassazione e la giurisprudenza nazionale, in precedenza, avevano già avuto modo di confrontarsi con le questioni legati alla permanenza delle notizie disponibili *online*, affrontando così incidentalmente il tema dell'oblio. Tuttavia, contrariamente alle conclusioni cui pervengono i giudici europei, la Suprema corte ha messo in luce come l'esigenza del diritto in questi casi non fosse quella di ottenere la mera dimenticanza delle informazioni contestate, quanto piuttosto quella di avere una loro corretta contestualizzazione, facendo di quest'ultima l'effettivo oggetto di pretesa (cfr. Cass. sez. III, civ, 5 aprile 2012, sent. n. 5525).

[457] Sul punto, è celeberrima ormai la sentenza *Google Spain*, da cui tra origine, per l'appunto, il c.d. *diritto all'oblio*, come diritto alla deindicizzazione rispetto ai risultati proposti sul proprio conto dai motori di ricerca. Il tema, peraltro, è stato ampiamente discusso in dottrina, in Italia e all'estero: M. BASSINI, *Google davanti alla Corte di giustizia: il diritto all'oblio*, in *Quaderni costituzionali*, n. 3, 2014, pp. 730 ss.; D. GRANARA, *Ricostruire il diritto all'identità personale: il diritto all'oblio e la libertà di informazione*, in *Diritto pubblico comparato*, n. 3/2014, pp. 1253 ss.; R. PARDOLESI, *L'ombra del tempo e (il diritto al) l'oblio*, in *Questione giustizia*, n. 1/2017, pp. 76 ss.; O. POLLICINO, *Un digital rights to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in *Diritto dell'informazione e dell'informatica*, 2014, pp. 569 ss.; B. PETKOVA, *Towards an Internal Hierarchy of Values in the EU Legal Order: Balancing the Freedom of Speech and Data Privacy*, in *Maastricht Journal of European and Comparative Law* 23 (3), 2016; G. SARTOR, *The right to be forgotten: Balancing interests in the flux of time*, in *International Journal of Law and Information Technology*, 24/2016; S. KULK, F. ZUIDERVEEN, N. BORGESIUS, *Privacy, freedom of expression, and the right to be forgotten in Europe*, in O. TENE, J. POLONETSKY, E. SELINGER (a cura di), *Cambridge Handbook of Consumer Privacy*, Cambridge, Cambridge University Press, 2017.

[458] Così A. MORELLI, *I diritti senza legge*, in *Consulta online*, 2015, pp. 23 ss.

[459] Reg. 679/2016, art. 17.

serie di condizioni limitative[460], volte a contemperare le aspettative di autonomia e riservatezza dell'interessato con le prerogative legate alla libertà di informazione, al diritto di difesa, all'interesse pubblico (soprattutto in ambito sanitario) e al corretto funzionamento delle attività archivistiche[461].

A questo si aggiunge poi il diritto alla portabilità dei dati[462]; un'altra novità pensata per venire incontro alle esigenze di protezione e controllo dettate dallo sviluppo della società dell'informazione. In una realtà in cui i dati personali possono essere utilizzati come «moneta di scambio»[463], questo diritto consente infatti all'interessato di ricevere in formato strutturato, di uso comune e leggibile da un dispositivo automatico, i dati personali che lo riguardano in precedenza forniti ad un

---

[460] *Ibidem*, § 1: «L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1».

[461] *Ibidem*, § 3: «I paragrafi 1 e 2 non si applicano nella misura in cui il 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; 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».

[462] Reg. 679/2016, art. 20.

[463] P. PACILEO, *Il diritto alla portabilità*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea sulla privacy*, Padova, Cedam, 2016, p. 227.

primo operatore. Così facendo, il *data subject* potrà trasmetterli ad un secondo titolare perché possano essere ulteriormente trattati, senza ulteriori incomodi.

Infine, è necessario soffermarsi sull'ultimo dei diritti sui *big data*, ossia il diritto di non essere sottoposti a una decisione basata unicamente sul trattamento automatizzato (inclusa la profilazione). Considerata la complessità dei processi con cui oggi i dati possono essere elaborati[464], l'art. 22 del regolamento sancisce innanzitutto diritto *negativo*[465], mettendo implicitamente in luce i rischi legati a questo tipo di procedimenti[466]. La disposizione prosegue quindi definendo una serie di condizioni che rendono ammissibili tali pratiche, fermo restando l'obbligo di adottare tutte le misure necessarie a garantire il corretto funzionamento dei sistemi e la sicurezza dei dati personali.

Rispetto a quanto previsto dalla direttiva, questa norma, in particolare, ha sollevato un accesso dibattito, soprattutto per quanto concerne la parte relativa al

---

[464] Come osservato, «attraverso queste prassi e con l'utilizzazione di algoritmi ormai molto raffinati, agli individui vien costruito un profilo su misura, una vera e propria identità digitale che misura le loro abitudini di consumo, di navigazione, la capacità di spesa, gli interesse e potenzialmente molti altri aspetti», in C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., p. 126; G. RESTA, *Identità personale e identità digitale*, in *Il diritto dell'informazione e dell'informatica*, 2007, pp. 511 ss.; A. SORO, *La società sorvegliata. I nuovi confini della libertà*, in Garante per la protezione dei dati personali (a cura di), *Atti del Convegno del 28 gennaio 2016*, pp. 5 ss.

[465] Reg. 679/2016, art. 22, § 1: « L'interessato ha *il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato*, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona».

[466] Gruppo Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679* (WP 251 rev. 01) del 6 febbraio 2018. Come si legge, infatti, «la profilazione può essere iniqua e creare discriminazioni, ad esempio negando l'accesso a opportunità di lavoro, credito o assicurazione oppure offrendo prodotti finanziari eccessivamente rischiosi o costosi. L'esempio seguente, che non rispetta le prescrizioni di cui all'articolo 5, paragrafo 1, lettera a), illustra come una profilazione iniqua può portare a proporre ad alcuni consumatori offerte meno interessanti rispetto ad altri» (p. 11). Allo stesso modo, le decisioni automatizzate possono avere diversi effetti pregiudizievoli in capo alla persona interessata, come, ad esempio, la cancellazione di un contratto; la concessione o alla negazione del diritto a una particolare prestazione sociale concessa dalla legge, come l'indennità di alloggio o le prestazioni per figli a carico; il rifiuto dell'ammissione in un paese o la negazione della cittadinanza (*ibidem*, p. 23).

c.d. «diritto ad una spiegazione» (*right to an explanation*)[467]. Richiamandosi all'ormai ben noto principio di trasparenza, infatti, secondo alcuni, il regolamento implicitamente abilita l'interessato a chiedere lumi sulla logica utilizzata dagli algoritmi che possono produrre effetti nella sua sfera giuridica, riconoscendo così un nuova pretesa alla piena "spiegabilità" (*explainability*) dei sistemi di calcolo.

Chiaramente, nella società dell'algoritmo, questa costituirebbe un'importante conquista di civiltà; un utilissimo meccanismo per assicurare la tutela dei diritti e dell'autodeterminazione informativa anche nell'utilizzo dei *big data* e dell'IA. Tuttavia, com'è logico ipotizzare, a queste pretese di trasparenza si contrappongono interessi altrettanto importanti, legati *in primis* alla tutela della proprietà intellettuale[468] e della sicurezza informatica. Si tratta quindi di un tema ancora fortemente dibattuto, sul quale ci sarà modo di tornare meglio in seguito.

### *e. La responsabilizzazione del titolare. Il principio di accountability*

Passando invece a considerare la posizione del titolare del trattamento e dei soggetti di cui si avvale e con cui collabora[469], il regolamento introduce un

---

[467] *Ex multis,* A. D. SELBST, J. POWLES, *Meaningful information and the right to explanation*, in *International Data Privacy Law*, 4/2017; pp. 233 ss.; S. WACHTER, B. MITTELSTADT, L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2/ 2017, pp. 76 ss.; J. A. KROLL , J. HUEY , S. BAROCAS , E.W. FELTEN , J.R. REIDENBERG , D.G. ROBINSON, H. YU *Accountable Algorithms*, in *University of Pennsylvania Law Review,* 165/2017, pp. 633 ss.

[468] Reg. 679/2016, *considerando* 63: « Ove possibile, il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali. Tale diritto non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software».

[469] È bene ricordare, infatti, come il trattamento dei dati personali oggi si snodi attraverso logiche assai complesse, che normalmente coinvolgono una pluralità di attori. Oltre ad avere normalmente la presenza di più contitolari del trattamento (reg. 679/2016, art. 26), questi possono avvalersi di diversi responsabili del trattamento (art. 28) o di propri rappresentanti (art. 27). A tutti questi, inoltre, si aggiunge la figura del responsabile della protezione dei dati personali (il c.d. *data protection officer,* o DPO), disciplinato invece alla sez. IV del capo IV.

importante cambiamento culturale, passando da una disciplina informata alle logiche di una serie di adempimenti formali ad una nuova mentalità improntata su un principio di derivazione anglosassone che pone al centro del sistema di garanzie il concetto di *accountability* (o responsabilizzazione)[470].

Senza dover più procedere alla notifica delle attività di trattamento all'Autorità di controllo, al titolare è lasciato un ampio margine di autonomia, purché questi sia in grado di dimostrare di aver adottato tutte le misure necessarie a garantire la sicurezza dei dati personali e la tutela dei diritti dell'interessato, intervenendo *ex ante* per ridurre e prevenire i possibili rischi legati alla sua attività[471].

Si afferma dunque una visione integrata del dovere di protezione (*duty of care*), rispetto al quale il *controller* è chiamato affrontare le problematiche legate ad ogni singola operazione in modo dinamico e relazionale, avvalendosi di diverse professionalità e competenze in campo informatico, giuridico e organizzativo[472].

Questa nuova filosofia si esplica dunque non solo nella responsabilità di *provvedere* ma anche nella responsabilità di *dimostrare* di aver adottato tutte le misure ragionevoli, tenuto 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»[473].

Il titolare è tenuto innanzitutto alla registrazione di ogni attività di trattamento posta in essere sotto la sua responsabilità[474], provvedendo a comunicare tempestivamente all'autorità di controllo competente tutti gli episodi di violazione

---

[470] Reg. 679/2016, art. 5, § 2.

[471] Circa la logica sulla prevenzione del rischio nell'ambito della protezione dei dati personali già si è detto richiamando I. BÖRÖCZ, *Risk to the Right to Protection of Personal Data*, cit.; R. GELLERT, *Understanding the notion of risk in the General Data Protection Regulation*, cit.; R. GELLERT, *Data Protection: a risk regulation? Between the risk management of everything and the precautionary alternative*, cit.; N. VAN DIJK, R. GELLERT, K. ROMMETVEIT, *A Risk to a Right? Beyond Data Protection Impact Assessment*, cit.

[472] G. FINOCCHIARO, *I quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in EAD. (diretto da), *Il nuovo regolamento europeo sulla privacy*, cit., p. 13.

[473] Reg. 679/2016, art. 32.

[474] *Ibidem*, art. 30.

dei dati (i c.d. *data breaches*) così da poter adottare subito i provvedimenti più adeguati[475]. Oltre a questi obblighi, sono previste inoltre una serie di garanzie volte a promuovere quest'approccio preventivo in termini pratici.

Tra queste rientrano senz'altro le strategie *by design* e *by default*, due locuzioni ormai diventate di uso comune con cui si indicano, rispettivamente, le misure atte ad integrare nel trattamento le garanzie a tutela degli interessati, nonché gli accorgimenti tecnici e organizzativi volti a limitare la portata quantitativa e qualitativa dei dati raccolti e trattati attraverso l'utilizzo di impostazioni predefinite[476].

Disciplinati *ex novo* nei primi due paragrafi dell'art. 25, il regolamento non fornisce una definizione specifica delle soluzioni che prescrive con questi requisiti, lasciando liberi i titolari di adottare le misure più opportune a secondo dalle specificità delle loro attività e del relativo contesto. Fatti alcuni accenni alle misure di pseudonimizzazione e minimizzazione dei dati[477], è interessante notare come, in questi casi, in linea con i principi di trasparenza e *accountability*, il legislatore europeo tenda a rifarsi a dei modelli aperti[478]. Così come in altri campi, anche in quest'ambito esistono specifici standard tecnici cui gli operatori, di volta in volta, possono rifarsi in funzione delle loro esigenze. Tuttavia, si è preferito orientarsi non tanto verso un unico standard prestabilito, quando ad un processo aperto e partecipativo, volto a stimolare il continuo miglioramento delle *best practices,* secondo un approccio calibrato in funzione delle esigenze del caso specifico.

---

475 *Ibidem*, artt. 33-34.

476 S. CALZOLAIO, L. FEROLA, V. FIORILLO, E.A. ROSSI, M. TIMIANI, *La responsabilità e la sicurezza del trattamento*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., pp. 173-174 ss.

477 Reg. 679/2016, art. 25, § 1: «[…] 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»

478 A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva*, in G. FINOCCHIARO (diretto da), *Il nuovo regolamento europeo sulla privacy*, cit., p. 307.

E proprio nell'ottica di anticipare il momento della tutela fin dalla fase di prima progettazione, a questi doveri si aggiungono le novità introdotte in merito alla valutazione di impatto sulla protezione dei dati. Essenzialmente, si tratta di un processo attraverso cui si opera una mappatura dei rischi, verificando le possibili conseguenze delle diverse attività sulle informazioni trattate e sui diritti dell'interessato, sia *ex ante* sia in corso d'opera[479].

Recependo prassi ormai consolidate in diversi settori, l'art. 35 prevede l'obbligo di procedere a questo genere di adempimento non per qualsiasi genere di trattamento, bensì soltanto per quelli che possono presentare un «rischio elevato per i diritti e le libertà delle persone fisiche».

Chiaramente i primi trattamenti sottoposti a questo tipo di valutazioni sono quelli che hanno ad oggetto operazioni in cui si elaborano su vasta scala grandi quantità di dati. In particolare, la norma prevede che questi accorgimenti siano necessari in almeno tre casi: (*a*) quando si effettui «una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche», (*b*) quando si proceda al «trattamento, su larga scala, di categorie particolari di dati personali» e (*c*) quando si predisponga «la sorveglianza sistematica su larga scala di una zona accessibile al pubblico».

Nelle linee guida predisposte dal Gruppo Articolo 29, peraltro, alla luce di quanto previsto dal testo normativo, si sono individuati ulteriori criteri per identificare le situazioni che necessitano di questi accorgimenti, includendo così anche i trattamenti che implichino la «creazione di corrispondenze o combinazione di insiemi di dati», l'utilizzo di «dati relativi a interessati vulnerabili», un «uso innovativo o [una] applicazione di nuove soluzioni tecnologiche od organizzative» e

[479] Art. 35

in ogni ipotesi in cui «il trattamento in sé impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto»[480].

Come rilevato, sebbene gli ordinamenti anglosassoni già avessero sviluppato da tempo dei validi sistemi di *privacy risk assessment*, la norma in questione si concentra non solo sulla riservatezza delle informazioni ma sulla protezione dei dati personali in senso ampio, idealmente aperto ad includere nella valutazione non solo le questioni inerenti il rispetto della dimensione informativa della vita privata, bensì un più ampio ventaglio di diritti.

Qualora dall'esito di tali operazioni emerga che il trattamento (o il sistema di trattamenti) in questione presenta un alto margine di rischio e il titolare non sia in grado di individuare autonomamente le soluzioni più appropriate, questi può consultarsi in via preventiva con l'Autorità di controllo per ottenere un parere sulle modalità più consone per contenere le eventuali minacce[481].

Nello svolgere tutte queste operazioni, il titolare, chiaramente, può collaborare e avvalersi di altri soggetti. Oltre alla possibilità di condividere responsabilità e obblighi con altri contitolari o con vari responsabili del trattamento, rispetto alle novità apportate dal regolamento, merita particolare attenzione la neo-introdotta figura del responsabile della protezione dei dati personali (o *data protection officer*)[482]. In alcuni casi, infatti, per assicurare al meglio la *compliance,* ci si dovrà avvalere della consulenza di un soggetto autonomo e altamente qualificato, cui spetta il compito di portare la cultura della *privacy* all'interno del contesto in cui opera e di promuovere

---

[480] Gruppo Articolo 29, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679* (WP248 rev.1) del 4 ottobre 2017, pp. 9-10.

[481] Reg. 679/2016, art. 36

[482] Reg. 679/2016, art. 37. Circa l'importanza di questa figura all'interno del nuovo sistema di tutele, si rinvia *ex multis* a S. CALZOLAIO, L. FEROLA, V. FIORILLO, E.A. ROSSI, M. TIMIANI, *La responsabilità e la sicurezza del trattamento*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., pp. 154 ss.; A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva*, in G. FINOCCHIARO (diretto da), *Il nuovo regolamento europeo sulla privacy*, cit., pp. 323 ss.; A. AVITABILE, *Il* Data Protection Officer*, ibidem*, pp. 331 ss.

l'adozione di ogni misura idonea alla protezione dei dati, tenendo i rapporti con le Autorità di controllo e interfacciandosi con gli interessati.

*f. Il ruolo delle Autorità di controllo e del Garante europeo*

È necessario, infine, dedicare qualche breve considerazione anche alle novità introdotte rispetto al ruolo e alle funzioni delle Autorità di controllo[483].

In questo ambito, la riforma si è mossa essenzialmente in due direzioni, potenziando da un lato gli strumenti di dialogo e coordinamento e dall'altro i poteri e le prerogative in capo ai singoli enti nazionali.

Quanto al primo di questi punti, va rilevato come, con l'istituzione di un modello di tutela unitario, il legislatore europeo, si sia premurato di istituire una serie di meccanismi atti a garantire un'applicazione omogenea della disciplina, potenziando i sistemi di cooperazioni tra le diverse Autorità[484].

A queste evoluzioni, chiaramente, hanno concorso una serie di fattori, primo tra tutti il tentativo di superare il criterio di stabilimento ai fini dell'applicazione del regolamento e, dunque, alla conseguente esigenza di incentivare un sistema di monitoraggio più capillare e diffuso, soprattutto rispetto ad attività di trattamento di carattere transfrontaliero e internazionale.

In questa prospettiva, nell'ottica di promuovere non solo la protezione ma anche la libera circolazione dei dati, è stata introdotta una prima grande semplificazione amministrativa attraverso l'istituzione di un sistema di sportello

---

483 E. GUARDIGLI, *Le Autorità di controllo*, in in G. FINOCCHIARO (diretto da), *Il nuovo regolamento europeo sulla privacy*, cit., pp. 489 ss.; A. PATRONI GRIFFI, *L'indipendenza del Garante*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., pp. 267 ss.

484 La sez. I del capo VII del reg. 679/2016 è dedicato infatti alla cooperazione tra le diverse Autorità di controllo, stabilendo particolari obblighi di cooperazione tra l'autorità di controllo capofila e le altre autorità di controllo interessate (art. 60) e di assistenza reciproca (art. 61); nonché definendo la disciplina per le c.d. operazioni congiunte (art. 62).

unico per le imprese (i c.d. meccanismi *one-stop-shop*)[485], in base al quale le imprese che svolgono la propria attività in diversi Stati dell'Unione possono rivolgersi all'Autorità in cui ha sede il loro stabilimento principale, senza così doversi interfacciare con una pluralità di soggetti, ciascuno per ogni diverso contesto. Sarà dunque tale Autorità (detta anche «capofila») a coinvolgere le altre interessate, e questo con l'intento di promuovere una più stretta collaborazione.

Quanto invece al potenziamento dei poteri di questi soggetti istituzionali, il regolamento non solo ribadisce il fatto che gli Stati membri debbano garantire *de iure* e *de facto* la loro indipendenza[486], ma potenzia il ruolo di questi figure dotandole di nuove prerogative (soprattutto sul fronte della tutela para-giurisdizionale) coinvolgendole appieno nel processo di responsabilizzazione dei titolari del trattamento. Come ricordato, infatti, in caso di violazione dei sistemi – e così della sicurezza dei dati trattati – il titolare, prima ancora di comunicarlo eventualmente agli interessati, è tenuto a segnalarlo all'Autorità di controllo, così da concertare subito, ove necessario, le successive strategie d'intervento. Allo stesso modo, il Garante collabora ad una perfetta *compliance* sul campo quando venga richiesto un parere preventivo, suggerendo le misure più consone per i trattamenti altamente rischiosi (o anche vietandoli del tutto).

### *4.2. La nuova strategia di data governance europea di fronte ai big data*

Alla luce delle considerazioni svolte finora, si può dunque pervenire ad alcune sommarie conclusioni. Come dimostrano le scelte operate in occasione del reg. 679/2016, a livello comunitario oggi si milita a favore di una strategia di *data*

---

485 Reg. 679/2016, *considerando* nn. 127 e 128, art. 56.

486 A. PATRONI GRIFFI, *L'indipendenza del Garante*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., pp. 267 ss.

*governance* forte, per veder affermate anche nel contesto digitale le garanzie essenziali a tutela dei diritti fondamentali e degli interessi di mercato.

A partire da questa prima proposta, la Commissione è andata poi a strutturare una nuova strategia di *data governance*, articolata e complessa, sfruttando a pieno le prerogative accordatele dal Trattato di Lisbona. Facendo leva proprio sulla piena costituzionalizzazione del diritto alla protezione dei dati personali a livello europeo, l'Unione, infatti, ha intrapreso un profondo processo di riforma, che tocca praticamente tutti gli ambiti in cui, in qualche modo, oggi si ha a che fare con questo tipo di contenuti.

Così com'era stato per la dir. 95/46, il nuovo regolamento generale è destinato a costituire la nuova «pietra miliare» dell'intera normativa, dettando così i principi generali cui andranno a rifarsi le diverse normative di settore. E in tal senso, ad una prima mappatura, possono già individuarsi quattro macro-aree di intervento, ognuna caratterizzata da alcune specifiche peculiarità.

In ordine cronologico, le prime a dover essere ricordate sono le due direttiva adottate contestualmente al reg. 679/2016, nell'ambito delle attività di cooperazione giudiziaria e di polizia in materia penale.

Nello specifico, si tratta, da un lato, della dir. UE 2016/680 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[487] e, dall'altro, della successiva dir. UE 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di

[487] Direttiva (UE) 2016/680 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 e che abroga la decisione quadro 2008/977/GAI del Consiglio.

terrorismo e dei reati gravi[488]; due normative accolte con particolare interesse dagli operatori e dalla dottrina, in quanto costituiscono il primo tentativo di definire una disciplina organica della materia in questi ambiti fino ad ora appannaggio esclusivo degli Stati membri.

Nonostante la materie escluse e le possibili deroghe alla disciplina comunitaria già sollevino alcune perplessità[489], l'adozione di queste due misure documentano un significativo passo avanti rispetto al quadro normativo preesistente[490]; un avanzamento reso possibile soprattutto dalle nuove competenze accordate alle istituzioni europee dall'art. 8 CDFUE e dall'art. 16 TFUE.

Sebbene infatti in quest'ambito, per l'intrinseca natura delle attività oggetto di regolamentazione, siano necessari alcuni particolari accorgimenti rispetto al normale tenore dei diritti tutelati da queste norme[491], la costituzionalizzazione della

---

[488] Direttiva (UE) 2016/681 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 nei confronti dei reati di terrorismo e dei reati gravi.

[489] Ad esempio, l'art. 1, § 3, dir. 2016/680, stabilisce che la medesima «direttiva non pregiudica la facoltà degli Stati membri di prevedere garanzie più elevate di quelle in essa stabilite per la tutela dei diritti e delle libertà dell'interessato con riguardo al trattamento dei dati personali da parte delle autorità competenti». Il successivo art. 2, § 3, in termini analoghi, prevede che: «la presente direttiva non si applica ai trattamenti di dati personali: *a*) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione; *b*) effettuati da istituzioni, organi, uffici e agenzie dell'Unione»; una formula particolarmente criptica, se si considera la natura della materia trattata e le relative competenze *de residuo* a livello nazionale. Non ultimo, l'art. 18, stabilisce che: «gli Stati membri possono disporre che i diritti di cui agli articoli 13, 14 e 16 siano esercitati conformemente al diritto dello Stato membro qualora i dati personali figurino in una decisione giudiziaria, in un casellario o in un fascicolo giudiziario oggetto di trattamento nel corso di un'indagine e di un procedimento penale».

[490] Per una panoramica, si rimanda a P. MILAZZO, *La direttiva UE 2016/680 e la protezione dei dati personali nell'ambito della sicurezza pubblica e della giustizia penale*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., pp. [709-722].

[491] La dichiarazione n. 21 allegata al Trattato di Lisbona, infatti, specifica che, per la particolarità del settore della cooperazione giudiziaria e di polizia, in questo settore è opportuno configurare un sistema di tutele specifico e appropriato alle esigenze specifiche delle attività svolte dalle varie autorità coinvolte, contemperando così le esigenze di tutela con i concorrenti interessi pubblici (Cfr. Dichiarazioni allegate all'atto finale della Conferenza intergovernativa che ha adottato il Trattato di Lisbona, 13 dicembre 2007, in *Gazzetta ufficiale dell'Unione europea,* 26 ottobre 2012, p. 347).

protezione dei dati personali ha permesso di ricondurre ad una tavola di valori unitari anche ambiti in precedenza estranei al diritto comune.

A queste prime iniziative, seguono quindi tre importanti novità. In primo luogo, vi è il reg. 2018/1725[492], un atto che introduce nuove misure di tutela in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, abrogando il precedente reg. 45/2001 e la decisione n. 1247/2002/CE[493]. A questo segue il reg. 2018/1807, volto a disciplinare il trattamento e libera circolazione dei dati non personali[494]; a riprova della centralità della componente informativa nell'economia globale ed europea. E infine, la direttiva 2019/790, la quale, riformando la disciplina sulla tutela della proprietà intellettuale[495] (materia storicamente complementare e contrapposto alla protezione dei dati personali nel settore digitale[496]) inquadra alcune importanti questioni legate al bilanciamento tra autodeterminazione informativa e diritti d'autore rispetto alla programmazione dei diversi *software*[497].

---

[492] Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio del 23 ottobre 2018 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE.

[493] Decisione n. 1247/2002/CE del Parlamento Europeo, del Consiglio e della Commissione del 1º luglio 2002 relativa allo statuto e alle condizioni generali d'esercizio delle funzioni di garante europeo della protezione dei dati.

[494] Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

[495] Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE.

[496] Come ricordano in modo emblematico la pronuncia della CGUE nella sent. 24 novembre 2011, *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, (causa C-70/10);

[497] In particolare, si veda quanto previsto dall'art. 28.

Segue quindi la proposta di un nuovo regolamento per sostituire la previgente normativa in materia di *e-privacy*[498] (intercettando anche in questi casi importanti questioni inerenti l'utilizzo dei *big data*[499]).

Al termine di questo breve itinerario, dunque, si può osservare come la strategia di *data governance*, anche grazie alle nuove competenze in materia, progressivamente si estenda ad ambiti e materie sempre più articolate ed estese, attirando il baricentro del sistema di tutele "verso l'alto", dal livello statale a quello comunitario.

Come osservato, considerata la natura dei *big data*, in cui la maggior parte dei contenuti consiste in dati personali, non sorprende che gli istituti relativi alla tutela di questa categoria valga a stabilire le regole dell'insieme[500]. E tuttavia, la logica con cui questo nuovo sistema di garanzie sta venendo conformandosi solleva più di qualche interrogativo: sul potenziale espansivo di questa nuova *law of personal data* in una realtà impregnata di informazioni; sui limiti che la normativa comunitaria incontra e sulle prerogative rimesse al legislatore nazionale in questa materia sempre più trasversale e sempre più europea; sulla natura del diritto alla protezione dei dati personali e sui rapporti che questo intrattiene con gli altri diritti fondamentali e sui differenti standard di tutela garantiti a livello nazionale ed europeo.

Tutti interrogativi cui si proverà a dare risposta nel capitolo seguente.

---

[498] Proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche) (Procedimento 2017/0003/COD - COM (2017) 10).

[499] Per una panoramica sul tema si rinvia a G. SCORZA, *Prospettive* de iure condendo *della protezione dei dati personali nel settore delle comunicazioni elettroniche, tra* Regolamento generale 2016/679 *e futuro* Regolamento e-Privacy, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., pp. 743 ss.

[500] R. D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 68.

# Capitolo 4

## Diritti fondamentali e *big data*
### *La protezione dei dati personali nel dialogo tra Corti*

### 1. Introduzione

Come accennato nell'introduzione, l'obiettivo di quest'ultimo capitolo è quello di rispondere al terzo punto in cui si articola il quesito di ricerca principale, ossia individuare le possibili risposte che oggi il diritto costituzionale è in grado di offrire per assicurare la tutela dei diritti fondamentali di fronte alla diffusione dei *big data*.

Per affrontare questo tema, tuttavia, è necessario soffermarsi ancora un istante sul fenomeno che si intende analizzare, chiarendo fin da subito il rapporto che si tende ad istaurarsi tra utilizzo dei c.d. «megadati» e protezione dei dati personali.

L'oggetto di studio, da un punto di vista materiale, rimane la c.d. «datificazione», ossia quel processo che – come già ricordato – consente di tradurre (o ridurre) ogni aspetto della realtà e dell'agire in termini informativi. È proprio osservando tale fenomeno, infatti, che si coglie come il concetto di dato personale abbia assunto una nuova rilevanza. Come rilevato, infatti, «ove si consideri che la parte di maggior rilievo della c.d. *data-sfera* è composta di dati personali – si coglie che – il principale presidio giuridico viene ad essere costituito dei relativi istituti di

tutela; al punto che porre le regole per questa sua componente può valere a stabilire le regole dell'insieme»[501].

In quest'ottica, dunque, le politiche promosse da Bruxelles nell'ambito della *data protection* possono essere intese come una sorta di movimento culturale. Il tentativo che si sta portando avanti, infatti, non è volto soltanto a fare della cultura dei diritti fondamentali uno dei pilastri fondanti del settore delle nuove tecnologie ma tende anche a incoraggiare la definizione di nuovi standard etici per uno sviluppo responsabile delle *data-intensive technologies*[502].

Le questioni legate all'autodeterminazione informativa e, più in generale, alla c.d. «funzione sociale» della protezione dei dati, dimostrano come le garanzie legate all'utilizzo delle informazioni – personali e non – si prestino ad avere implicazioni di ampio respiro, intercettando tutti i diritti e gli interessi che, direttamente o indirettamente, hanno a che fare con le operazioni di trattamento. Fin da principio, è emerso in modo chiaro come da un corretto esercizio del potere informativo non dipendano soltanto delle legittime aspettative sulla riservatezza dei contenuti, bensì anche implicazioni di più ampio respiro, fino ad intaccare le garanzie minime della *rule of law*. Attorno ai processi informativi, infatti, gravitano da sempre una pluralità di interessi – pubblici e privati, individuali e collettivi – intercettando principi e diritti assai diversi tra loro, rispetto ai quali le attività di trattamento risultano essere del tutto strumentali.

In una realtà «guidata dai dati», chiaramente, queste considerazioni sono destinate ad acquisire rilievo crescente, amplificandosi. La protezione dei dati personali, come *diritto* fondamentale, non risulta più finalizzato al solo rispetto della

---

[501] R. D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit. p. 68.

[502] Paradigmatiche in tal senso sono le iniziative intraprese per promuovere uno sviluppo etico dell'intelligenza artificiale, come dimostrano i lavori del Gruppo indipendenti di esperti ad alto livello sull'intelligenza artificiale, istituito dalla Commissione europea nel giugno 2018, *in primis* il documento *Orientamenti etici per un IA affidabile* (8 aprile 2019).

vita privata ma è destinata a legarsi ad una pluralità di altri interessi, facendo così dell'art. 8 CDFUE un insieme di garanzie preordinate e necessarie alla tutela di *tutti* i diritti fondamentali oggi intercettati dall'utilizzo dei dati (dalla libertà di espressione alla tutela della proprietà intellettuale, dal diritto alla sicurezza al principio di trasparenza, fino ad includere le garanzie di dignità ed eguaglianza poste a presidio del principio personalista). Allo stesso modo, la *disciplina* sulla protezione dei dati personali promette di avere un campo di applicazione vasto e trasversale, intercettando ambiti in precedenza orientati ad altre logiche e attraendo questioni prima decise a livello nazionale nell'orbita delle politiche comunitario.

Di fronte a questo scenario, dunque, non possono non emergere delle perplessità. Se è vero che il sindacato sui diritti fondamentali a livello europeo si ispira ai principi derivanti dalle tradizioni costituzionali comuni, rimane impregiudicato il fatto che, a seconda del contesto, ai medesimi interessi possano essere garantiti tutele di diversa intensità.

E tutto ciò risulta quanto mai evidenti in una materia come la protezione dei dati personali, in cui l'intera disciplina gravita attorno all'esigenza di bilanciare interessi e aspettative contrapposte. È per questo che, nelle pagine che seguono, si tenterà di approfondire il complicato rapporto tra diritto nazionale e diritto europeo in questo ambito, prendendo in considerazione alcune specifiche questioni.

In primo luogo, si andrà ad approfondire l'ambito di applicazione e la plasticità della definizione di dato personale. Questa, infatti, da un punto di vista pratico, costituisce uno dei presupposti essenziali per vedere ricondotta una questione alla relativa disciplina (e così, il più delle volte, nel novero delle competenze del giudice comunitario). L'obiettivo quindi è quello di esaminare con attenzione quello che si potrebbe definire il «coefficiente elastico» di tale concetto in un contesto sempre più *data-driven*, per vedere come il processo di datificazione contribuisca *de facto* ad una graduale europeizzazione della tutela dei diritti rispetto all'utilizzo dei *big data*.

A completamento di queste prime considerazioni, in seguito, si prenderanno in considerazione i limiti che tradizionalmente la normativa comunitaria incontra in questa materia e le prerogative ancora riconosciute al legislatore nazionale per le questioni di interesse statale. Si analizzerà come la Corte di giustizia UE, nel tempo, sia andata progressivamente a circoscrivere la portata di tali clausole nell'ottica di promuovere una *digital rule of law* europea. In questo caso, l'analisi ha lo scopo di mettere in luce come i giudici europei – anche in questi frangenti – siano propensi ad una lettura estensiva delle proprie competenze, spesso considerandosi l'ultima voce legittimata a pronunciarsi sul rapporto tra dati e diritti anche in materie particolarmente sensibili per gli Stati membri.

Sulla base di queste premesse, si andranno quindi ad approfondire i rapporti che legano la protezione dei dati personali agli altri diritti fondamentali tutelati dalla Carta di Nizza, indagando la gerarchia di valori promossa a livello europeo sulla base dell'art. 8 CDFUE. L'intento è quello di evidenziare le logiche che guidano la CGUE nell'adempiere a questo suo nuovo ruolo di garante costituzionale dei diritti digitali, evidenziando come, in alcuni casi, gli argomenti utilizzati si possano discostare dalla diversa sensibilità dei giudici nazionali.

Al termine del percorso, ci si concentrerà sulla dimensione rimediale, avendo a mente soprattutto le questioni legate all'accessibilità dei dati e alla comprensibilità delle logiche sottese alle operazioni di trattamento più sofisticate. In particolare, si approfondirà il rapporto tra protezione dei dati e trasparenza del processo decisionale. Ci si soffermerà soprattutto sul potenziale delle garanzie introdotte dall'art. 22 e dal *considerando* 71 del nuovo regolamento e i margini di discrezionalità concessi ai legislatori locali su questo tema, "testando" l'attuale stato dell'arto in questo difficile sistema di tutele integrate.

## 2. Certezza del diritto, dati personali e *big data*

Si da principio, l'obiettivo della disciplina sulla protezione dei dati personali è stato quello di offrire nuove certezze inerenti la tutela dei diritti fondamentali intercettati dall'utilizzo dei dati personali.

Ragionando sui contenuti minimi di questa normativa, ci si aspetta, ad esempio, la possibilità di conoscere l'esistenza del trattamento, l'identità dei soggetti coinvolti, la natura dei dati utilizzati, le logiche del procedimento. A seconda dei casi, l'interessato potrà esercitare specifici diritti, facendo i suoi interessi quanto alla propria autoderminazione informativa. Il titolare del trattamento, per contro, sarà tenuto ad adottare tutte le misure tecniche necessarie per garantire la sicurezza delle operazioni da lui svolte, conformando la propria attività secondo quanto previsto legge.

Tutto questo si basa su un premessa apparentemente elementare, ossia il fatto che i dati in questione siano riconducibili alla categoria dei *dati personali*, secondo la definizione che di questo concetto è offerto dalla normativa.

La diffusione dei *big data analytics*, tuttavia, ha messo a dura prova la tenuta di questo postulato. In una realtà in cui in ogni istante vengono prodotte enormi quantità di dati, aggregati e trattati secondo logiche articolate e complesse, la tenuta di questa tradizionale distinzione che suole differenziare tra dati personali risulta infatti seriamente compromessa[503].

La maggior parte delle tecnologie di cui comunemente ci si avvale, infatti, normalmente prevede un'interazione uomo-macchina, e anche quando i sistemi sono tra loro connessi senza la necessità di un'interdipendenza diretta con l'utente, i risultati del processo svolto automaticamente dai dispositivi tende ad orientare i

---

[503] A. MANTELERO, *La privacy* all'epoca dei *Big Data*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 1190; N. PURTOVA, *The law of everything. Broad concept of personal data and future of EU data protection law,* in *Law, Innovation and Technology*, 2018.

propri criteri d'azione verso la realizzazione di un risultato umanamente apprezzabile. I dati utilizzati, dunque, anche quando non siano qualificabili come contenuti *personali* nel senso più immediato e intuitivo del termine, in ultima possono comunque finire col riguardare una certa persona.

In questo modo, dati che potrebbero definirsi neutri, se correlati ai contenuti di altri *dataset,* possono fornire informazioni anche molto specifiche rispetto al singolo, così come ad intere categorie di persone (basti pensare a quel che abilmente dimostrano le operazioni di profilazione). Ugualmente, proprio per la quantità di contenuti oggi a disposizione, dati resi anonimi possono essere facilmente re-identificati (almeno in parte) anche attraverso l'utilizzo di tecniche non particolarmente costose.

Prima di passare ad analizzare il rapporto tra l'art. 8 CDFUE e gli altri diritti fondamentali sanciti dalla Carta, è quindi necessario indagare come oggi si tenda ad interpretare la disciplina sulla protezione dei dati personali, andando a verificare se e come tale normativa si presti a far fronte alla complessità di fondo introdotta dalla datificazione.

### *2.1. Dati (o informazioni?) personali e tutela dei diritti al tempo dei big data*

Prima di addentrarsi in un'attenta analisi delle definizioni giuridiche, è utile spendere qualche istante per delle brevi premesse sulla tecnica normativa con cui possono essere elaborate queste nozioni, e così sull'elaborazione del concetto di «dato personale».

Per approfondire gli impatti sociali delle tecnologie digitali molte discipline umanistiche hanno iniziato ormai da tempo ad elaborare una nuova cornice

concettuale, escogitando i modi e le forme più opportune per assimilare nozioni e logiche tecniche all'interno dei propri domini di riferimento[504].

In ambito giuridico si è sviluppato un percorso analogo. Come dimostrano anche le prime leggi sulla protezione dei dati, il legislatore ha accolto questo cambio di passo cominciando ad introdurre una serie di garanzie pensate specificamente per la tutela dei contenuti informatizzati, delineando così un nuovo sistema di garanzie che progressivamente si è affrancato dalla storica normativa sulla tutela degli archivi e dei documenti cartacei.

Da un punto di vista teorico, tuttavia, quest'operazione di rinnovamento nel tempo continua a riproporre alcuni passaggi particolarmente critici. A differenza di quel che accade in altri contesti, il linguaggio giuridico non ha soltanto natura descrittiva, ma anche – e soprattutto – prescrittiva. Ciò implica che nel momento in cui ci si accinga a trasporre dei concetti tecnici, dal perimetro delle definizioni vengano poi a delinearsi obblighi e diritti, abilitando i diversi soggetti coinvolti ad adeguare il loro agire in funzione di quanto previsto dalla norma.

Per questo motivo, nell'evoluzione della disciplina sui dati personali, le scelte terminologiche sono state oggetto di attenta riflessione[505]. Come la giurisprudenza dimostra ormai da tempo, l'innovazione suggerisce l'utilizzo di nozioni flessibili, in grado di assecondare lo sviluppo tecnologico senza incorrere in una rapida obsolescenza[506]. Allo stesso modo, però, la plasticità di questi concetti può generare situazioni di grave incertezza, in quanto il potenziale espansivo di tali definizioni

---

[504] L. FLORIDI, *La rivoluzione dell'informazione*, Torino, Codice Editore, 2012.

[505] Come dimostra l'analisi svolta da Van Alsenoy, con riferimento – ad esempio – all'evoluzione dei concetti di dato personale, titolare del trattamento e responsabile del trattamento. (Cfr. B. VAN ALSENOY, *Data Protection Law in the EU: Roles, Responsibility and Liability*, cit., pp. 325 ss.)

[506] L.A. BYGRAVE, *Information Concepts in Law: Generic Dreams and Definitional Daylight*, in *Oxford Journal of Legal Studies*, 2015, pp. 91-205, spec. pp. 92-93.

spesso concorre a rendere ambiguo il significato delle medesime, creando perplessità nei destinatari[507].

Chiaramente, si tratta di un problema trasversale, che non interessa soltanto la disciplina sulla protezione dei dati personali, bensì tutte le normative che regolano i settori tecnico-scientifici caratterizzati da forti processi innovativi.

Tuttavia, nell'ambito della materia che qui ci occupa, questa tendenza si avverte in modo particolarmente marcato, tanto che nel tempo definizioni rimaste formalmente invariate hanno avuto bisogno di numerosi interventi per essere prontamente riadattate allo sviluppo delle tecnologie e del contesto circostante[508]. Come ricordato, il presupposto essenziale per dare attuazione a questa disciplina rimane il fatto che i contenuti trattati possano essere qualificati come elementi di «carattere personale»; tant'è che anche questo concetto, negli anni, ha avuto bisogno di varie precisazioni.

Ripercorrendo l'evoluzione della normativa, si può osservare come la scelta di circoscrivere l'ambito di applicazione di queste garanzie in tal senso non è stata una scelta ovvia. In principio, il legislatore nazionale in alcuni casi (come, ad esempio, quella del *Land* dell'Assia) aveva optato per una definizione neutra, includendo nell'ambito di applicazione della disciplina *tutte* le attività di trattamento che in qualche modo fossero in grado di produrre effetti giuridici rilevanti nella sfera di interesse degli individui coinvolti[509]. Quest'approccio, tuttavia, è stato poi

---

[507] *Ibidem*.

[508] Per capire appieno la portata del problema, basta osservare come molte operazioni prima svolte in modalità analogica oggi sono state convertite in forma digitale, moltiplicando così le attività di trattamento. A queste si aggiungano poi gli innumerevoli processi con cui in ogni istante vengono elaborate enormi quantità di informazioni; prova ne sono i motori di ricerca, i *social network* e le piattaforme online piuttosto che i sistemi di geo-localizzazione di uso più comune. In quest'ottica, dunque, vanno letti pareri prodotti negli anni dal Gruppo Articolo 29 per ridefinire la portata di alcuni concetti o per specificare il contenuto della disciplina rispetto allo sviluppo di nuovi servizi (si vedano, in particolare, il parere n. 4/2007 sul concetto di «dato personale» (WP136); il n. 1/2010 sui concetti di titolare e responsabile del trattamento (WP169)).

[509] B. VAN ALSENOY, *Data Protection Law in the EU: Roles, Responsibility and Liability*, cit., p. 166; S. RODOTÀ, *Tecnologie e diritti*, cit.

abbandonato per lasciare spazio alle nozioni che conosciamo. In diversi ordinamenti, infatti, il legislatore si è concentrato soprattutto sulla possibilità di tracciare dei parallelismi tra la preesistente disciplina sulle informazioni e la nuova normativa sulla protezione dei dati, spesso utilizzando figure pensate per una realtà "analogica".

Sebbene quindi il concetto di «dato personale» sia ormai comunemente invalso, una più attenta analisi linguistica rivela alcune criticità nel modo in cui questa nozione è concepita. Nonostante, infatti, in ambito giuridico termini come «dato» e «informazione» vengano utilizzati come se fossero sinonimi, da un punto di vista tecnico le due parole indicano contenuti ben diversi e difficilmente sovrapponibili.

In ambito informatico, quando si parla di «informazione» normalmente si utilizza una definizione generale che associa a questo concetto due diverse componenti: da un lato i *dati*, dall'altro il *significato*[510]. L'informazione, cioè, risulta «*costituita di dati* – in una – sintassi figurale [che] rende l'illustrazione potenzialmente dotata di significato per l'utente»[511]. Da un punto di vista logico, dunque, tra i due termini viene a delinearsi un rapporto di strumentalità che non consentirebbe alcun tipo di sovrapposizione.

In ambito giuridico, invece – come si accennava poc'anzi – non è infrequente che queste due espressioni vengano utilizzate come se fossero interscambiabili. E tale prassi che è stata spiegata secondo logiche diverse. Per alcuni autori, una simile scelta è giustificata dal fatto che le due parole – "dato", "informazione" –sono dotate di un significato essenzialmente auto-evidente e dunque, anche da un punto

---

[510] Come spiegato in L. FLORIDI, *La rivoluzione dell'informazione* (Torino, Edizioni Codice, 2012, p. 25) la definizione generale di informazione (DGI) è espressa infatti secondo una formula tripartita secondo cui (*s*) è un'istanza di informazione compresa come contenuto semantico, se e solo se: (*1*) DGI.1: (*s*) consiste di *n* dati, per cui $n \geq 1$; (*2*) DGI.2: i dati sono *ben formattati*; (*3*) DGI.3: i dati ben formattati sono *dotati di significato*.

[511] *Ibidem*.

di vista giuridico, non abbisognano di ulteriori differenziazioni[512]. Secondo altri, invece, la scelta di ricorrere ad un linguaggio generico risponde ad un fine specifico ossia quello di rendere più stabile la disciplina, permettendo di adattare le definizioni alle future evoluzioni della tecnologia[513].

Analizzata alla luce di queste considerazioni, dunque, la definizione di «dato personale» dimostra alcuni punti di fragilità. Leggendo la norma di riferimento, infatti, si osserva come possa essere considerata tale «*qualsiasi informazione* riguardante una persona fisica identificata o identificabile»[514], con un evidente inversione logica dei termini. Cionondimeno, la normativa europea ha adottato un approccio generalista e, includendo nell'ambito di applicazione sia i trattamenti automatizzati sia quelli tradizionali, ha optato per delle scelte linguistiche idonee ad entrambe le tipologie di contenuti (anche a discapito della specificità del lessico tecnico).

Per questo motivo, a fronte dei successivi sviluppi tecnologici, queste definizioni hanno richiesto numerose specificazioni e adattamenti, necessari a chiarire di volta in volta la portata del concetto in esame davanti alla crescente granularità dei dati a disposizione. Nuove tecniche di trattamento, infatti, consentono di elaborare e trattare diversi tipi di contenuto, fino manipolarne le caratteristiche e la descrittività anche in modo relativamente economico[515].

Sono così emersi alcune importanti interrogativi circa l'attuale perimetro della definizione di «dato personale», anche perché da quest'ultima dipendono in larga parte i presupposti per la successiva applicazione dell'intera disciplina. Se, per un verso, risulta evidente come la «datificazione» di procedimenti complessi possa

---

[512] L.A. BYGRAVE, *Information Concepts in Law: Generic Dreams and Definitional Daylight*, cit. pp. 92-93.

[513] *Ibidem.*

[514] Reg. 679/2016, art. 4, n. 1.

[515] Tanto ne è prova il fatto che attorno a questo tipo di operazioni oggi graviti un intero settore di mercato: il c.d. *data brokering*. Cfr. A. MANTELERO, *La privacy* all'epoca dei *Big Data*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 1190;

comportare gravi rischi[516] – non solo per quanto riguarda la *privacy*, ma anche per altri valori essenziali quali l'uguaglianza e il pluralismo[517] – dall'altro risulta difficile capire se la *data protection* sia idonea garantire adeguati livelli di tutela rispetto allo sfruttamento dei *big data*, e questo proprio per l'ambigua natura di questi *dataset.*

Stando così le cose, dunque, si tratta di verificare innanzitutto in che termini questa normativa possa effettivamente rispondere ai problemi appena accennati, verificando la plasticità del concetto in esame.

In tutto questo, peraltro, bisognerà tenere in considerazione un ulteriore risvolto, forse meno immediato. Maggiore è infatti il perimetro della definizione di dato personale, maggiore risulta l'ambito di applicazione della relativa disciplina. Considerato che oggi la maggior parte delle attività di *routine* presuppone l'utilizzo dei dati, c'è da chiedersi, quindi, quale sia destinata ad essere la vocazione di questa normativa, e così l'influenza del diritto comunitario nel disciplinare le diverse fattispecie che possono essere ricondotte in quest'alveo.

---

[516] Circa la dimensione del rischio e l'approccio preventivo all'utilizzo delle tecnologie dei dati, questo è un orientamento che si registra già dalle prime riflessioni in materia di protezione dei dati personali (Cfr. Cfr. F.W. HONDIUS, *Emerging Data Protection in Europe*, Amsterdam-Oxford, New York, 1975, p. 7). Quest'impostazione, peraltro, è stata fortemente enfatizzata nell'ambito del nuovo reg. EU 679/2016 (di cui si dirà a breve) che, all'art. 35, affronta proprio le questioni legate alla valutazione di impatto. Circa il tema del rischio in materia di protezione dei dati personali, in particolare, v. I. BÖRÖCZ, *Risk to the Right to Protection of Personal Data*, in *EDPL*, 4, 2016; R. GELLERT, *Understanding the notion of risk in the General Data Protection Regulation*, in *Computer Law and Security Review*, 2017; R. GELLERT, *Data Protection: a risk regulation? Between the risk management of everything and the precautionary alternative*, in *International Data privacy Law*, 5, 2015; N. VAN DIJK, R. GELLERT, K. ROMMETVEIT, *A Risk to a Right? Beyond Data Protection Impact Assessment*, in *Computer Law and Security Review*, 32, 2016.

[517] J. PODESTA et al., *Big Data: Seizing Opportunities, Preserving Values,* White House, Executive Office of the President, maggio 2014; C. MUÑOZ, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights,* White House, Executive Office of the President, maggio 2016; *#BigData: Discrimination in data-supported decision making,* EU Fundamental Rights Agency, maggio 2018; EDPS, *Meeting the challenges of big data A call for transparency, user control, data protection by design and accountability,* parere 7/2015; EDPS, *EDPS Opinion on coherent enforcement of fundamental rights in the age of big data,* parere 8/2016; EDPS, *EDPS Opinion on online manipulation and personal data*, parere 3/2018. In dottrina, *ex multis,* alcuni spunti in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018.

Per affrontare questi interrogativi non rimane che analizzare la portata del dato normativo, esaminando l'attuale statuto giuridico dei dati nell'ambito del reg. 679/2016. Alla luce di quanto emerso, si andrà a testare il "coefficiente elastico" di questa definizioni. Si indagherà soprattutto come negli anni la Corte di giustizia abbia promosso una lettura estensiva del concetto, attraendo così nell'orbita del diritto comunitario diverse questioni in precedenza disciplina dal diritto nazionale.

### *2.2. Una breve ricognizione sull'attuale statuto giuridico dei dati nel reg. 679/2016*

Da un punto di vista logico, il fatto che esista la categoria dei dati personali, presuppone che vi siano anche dati non riconducibili a tale insieme, ossia dei dati non-personali. Questa dicotomia oggi ha cominciato a farsi spazio anche sul piano del diritto, tanto che non solo si è cominciato disciplinare anche la circolazione dei *non-personal data*[518] ma lo stesso reg. 679/2016 presta particolare attenzione alle diverse tecniche con cui è possibile graduare la "personalità" del dato, definendo una specifica disciplina per i dati c.d. pseudonimizzati.

Come suggerito da alcuni, alla luce delle tecniche con cui oggi dati possono essere manipolati e modificati, la tradizionale dicotomia tra dati personali e dati anonimi è dunque destinata a subire dei temperamenti, adottando «un'impostazione che vede il dato personale e quello anonimo come poli estremi di una scala graduale caratterizzata da un crescente livello di anonimizzazione»[519].

Alla luce di queste premesse, dunque, si deve tentare di chiarire il significato e i contenuti di queste tre categorie.

---

[518] Proposta di Regolamento del Parlamento europeo e del Consiglio, relativo a un quadro applicabile alla libera circolazione dei dati non-personali nell'Unione europea del 13 settembre 2017 (riferimenti disponibili a questo link, visitato il 30.12.18)

[519] A. MANTELERO, *La privacy* all'epoca dei *Big Data*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 1191.

*a. Dati personali* – Ovviamente il punto di partenza non poteva non essere la categoria dei dati personali.

Di questa definizione si trovano alcuni chiari cenni già nelle prime leggi in materia[520]. Così come in precedenza, infatti, ci si era concentrati sulla protezione dei documenti e dei fascicoli personali, salve poche eccezioni[521], la normativa storicamente ha limitato il proprio ambito di applicazione solo alle informazioni sul singolo individuo.

Il regolamento, dunque, considera dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile», ritenendo «identificabile la persona fisica che può essere identificata, direttamente o indirettamente»[522].

Analizzando la seconda parte della disposizione e comparando il testo attuale con quello della precedente direttiva, si avverte peraltro come ci si trovi di fronte ad un concetto in continua evoluzione. Nel catalogo di possibili identificativi rilevanti ai fini della disciplina, si trova infatti una casistica ben più estesa che in passato, aggiungendo ai tradizionali riferimenti all'«identità fisica, fisiologica, psichica, economica, culturale o sociale» anche i dati genetici e biometrici, quelli relativi all'ubicazione e gli identificativi online[523].

Quest'evoluzione documenta come ci si trovi di fronte ad una nozione che si presta ad un'interpretazione estensiva, in grado di includere nel proprio perimetro i diversi elementi che nel tempo sono risultati meritevoli di tutela[524].

---

[520] Questi concetti, infatti, sono stati definiti chiaramente sia dalla legge svedese del 1973, dalla legge francese del 1976 e dalla legge federale tedesca del 1974. F.W. HONDIUS, *Emerging Data Protection in Europe*, Amsterdam-Oxford, New York, 1975; D.H. FLAHERTY, *Protecting Privacy in Surveillance Societies. The Federal Republic of Germany, Sweden, France, Canada, and the United States*, Chapel Hill (NC), 1989.

[521] Come, ad esempio, la legge del *Land* dell'Hesse del 1970 (B. VAN ALSENOY, *Data Protection Law in the EU*, cit., p. 166 ss.).

[522] Cfr. Reg. UE 679/2016, art. 4(1) (parte prima); dir. CE 46/95, art. 2, lett. a. (prima parte).

[523] Cfr. Reg. UE 679/2016, art. 4(1) (parte seconda); dir. CE 46/95, art. 2, lett. a. (prima seconda).

[524] V. in seguito, §§ 4-5 e relativi riferimenti in nota.

Com'è evidente, però, continuano ad affiorare alcune criticità legate all'uso indifferenziato di "dato" e "informazione"; una questione di non poco conto se si ricorda che la protezione dei dati personali spesso sembra l'unico rimedio per ottenere tutela dei diritti "digitali".

C'è da chiedersi, quindi, per quali motivi questa definizione tenda ad essere interpretata in modo così creativo: se per dare un'applicazione coerente alla normativa nel suo insieme oppure per estendere certe garanzie a situazioni che altrimenti ne rimarrebbero sprovviste. Vista però la centralità del tema, su questo punto si tornerà meglio più avanti, quando il quadro normativo sarà più chiaro anche rispetto alle altre categorie di dati.

*b. Dati pseudonimizzati* – Qui più che di "dati", sarebbe opportuno parlare di "tecniche". Il reg. UE 679/2016, infatti, prevedendo l'obbligo di adottare specifiche misure di protezione by design e by default[525], ha introdotto la nozione di "pseudonimizzazione"[526], permettendo così di individuare indirettamente una seconda specie di dati.

La peculiarità degli elementi trattati con queste modalità è quella di non poter «più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive»[527].

In altri termini, ci si trova di fronte ad una categoria intermedia, in cui l'utilizzo della tecnologia permette di mitigare volontariamente il carattere personale dei contenuti. Questi espedienti, però, non sono volti a sottrare i dati all'applicazione del regolamento, poiché la norma presuppone che il titolare continui

---

[525] Reg. UE 679/2016, art. 25. In dottrina, *ex multis,* L.A. BYGRAVE, *Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements*, in *Oslo Law Review*, 2/2017; G. D'ACQUISTO, M. NALDI, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, 2017.

[526] Reg. UE 679/2016, art. 4(5).

[527] *Ibidem*.

a conservare le informazioni aggiuntive a parte, adottando le debite cautele[528]. Il ricorso a queste misure mira piuttosto a modulare gli obblighi in capo al *controller* in funzione dell'effettiva entità del rischio legato al trattamento: l'utilizzo dei dati, infatti, non richiede che questi vengano sempre elaborati in forma identificativa e, peraltro, minimizzando la personalità degli stessi, si riducono sensibilmente i problemi legati alla confidenzialità delle informazioni.

Tuttavia, se il titolare non ha bisogno di utilizzare dati identificativi, il regolamento stesso prevede che non sia tenuto a conservarne altri solo al fine di rendere applicabile la relativa disciplina[529], ammettendo così che in alcuni casi si possa smettere di conservare le informazioni aggiuntive.

Rispetto a queste modalità di trattamento, emerge quindi una prima perplessità. Le dinamiche legate all'utilizzo dei dati spesso non vedono un unico titolare, bensì l'attività coordinata di diversi soggetti che intervengono nel processo con poteri e responsabilità molto diverse[530]. Nei diversi passaggi, dunque, non è escluso che, mancando delle informazioni necessarie, il singolo controller possa non essere in grado individuare il soggetto.

Di fronte a questa eventualità, potrebbero quindi venirsi a creare situazioni ambigue, in cui l'interessato non è più nelle condizioni di esercitare alcuni suoi diritti sui dati a meno che non si provveda ad integrare questo gap identificativo di cui si trova ad essere oggetto[531].

Tutto ciò considerato, dunque, si vede come già con questa prima differenziazione si incontrino non pochi problemi, lasciando aperti sensibili margini di incertezza nell'applicazione della disciplina, così come per la tutela dei diritti.

---

528 *Ibidem*.
529 Reg. UE 679/2016, art. 11, § 1.
530 B. VAN ALSENOY, *Data Protection Law in the EU*, cit., p. 76 ss.
531 Reg. UE 679/2016, art. 11, § 2.

*c. Dati anonimi e dati non-personali* – Le perplessità emerse rispetto all'utilizzo delle tecniche di pseudonimizzazione portano così alle questioni legate ai dati anonimi. Il motivo per cui, tuttavia, questi vengono analizzati assieme ai dati non-personali potrebbe essere meno evidente. La scelta è legata al fatto che, rispetto a queste due categorie, il reg. 679/2016 non offre una definizione vera e propria dei diversi contenuti e accorpa entrambi i concetti in un'unica disposizione, nell'ambito dei *considerando*.

Sono qualificate come "anonimi" i «dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato» così come le «informazioni che non si riferiscono a una persona fisica identificata o identificabile» (i non-personali)[532]. Da un punto di vista di politica normativa, la caratteristica che accomuna i due concetti è che in entrambi i casi – sia per i dati anonimi, sia per quelli non-personali – i principi e la disciplina del regolamento non trovano applicazione[533].

Pensando soprattutto allo sviluppo delle tecnologie data-intensive, tuttavia, questa soluzione crea qualche problema.

Sul piano giuridico, infatti, si ritiene che i dati non possano essere de-identificati in modo definitivo[534], poiché la loro "personalità" rimane sempre legata ad una componente relazionale. Oltre agli elementi di partenza, cioè, vanno considerate anche le tecnologie e le altre informazioni di cui il titolare può disporre a tal fine[535]. Contrariamente a quanto potrebbe sembrare, si finisce col concludere che una completa de-personalizzazione risulta teoricamente impossibile; si potrà

---

[532] Reg. UE 679/2016, cons. 26.

[533] *Ibidem:* «*I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime*».

[534] Gruppo Articolo 29, *Parere 5/2014 sulle tecniche di anonimizzazione,* WP216, 10 aprile 2014.

[535] Reg. UE 679/2016, cons. 26: «*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*».

procedere soltanto ad una valutazione probabilistica, considerando la possibilità che il soggetto possa essere di nuovo individuato[536].

Un simile ragionamento sembrerebbe quindi escludere che si possa anche solo ipotizzare l'esistenza di una categoria di dati assolutamente non-personali. Utilizzando quest'approccio relazionale, infatti, in astratto anche i contenuti che per natura non avrebbero nulla di personale (dati ambientali, operativi, etc.[537]) in qualche modo potrebbero comunque essere ricondotti ad un individuo specifico, finendo così col gravitare sempre nell'orbita della personal data protection[538].

Viene quindi da chiedersi che effetti producano sul piano del diritto quelle misure che, da un punto di vista tecnico, vengono intese come una completa anonimizzazione dei dati e, per contro, come debbano regolarsi quei soggetti che di norma trattano dati non-personali.

Evidentemente, rispetto a queste ultime due categorie, la situazione risulta quanto mai confusa. Ancora una volta, infatti, appare chiaro come il termine di paragone rimanga il concetto di dato personale, lasciando ad ogni altra definizione uno spazio marginale ed incerto. Di fronte allo sviluppo delle tecnologie *smart*, quindi, ci si chiede se queste innovazioni basate sull'utilizzo dei dati saranno sempre destinate a ricadere nell'ambito di applicazione del reg. UE 679/2016 o se, invece, possano essere assoggettate ad altre discipline pur senza pregiudicare la tutela dei diritti[539].

---

[536] Reg. UE 679/2016, cons. 26: «*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*».

[537] L. FLORIDI, *La rivoluzione dell'informazione*, cit., 23 ss.

[538] N. PURTOVA, *The law of everything*, cit. p. 57.

[539] In tal senso, anche chi si fosse aspettato maggior chiarezza dalla proposta di regolamento sulla libera circolazione dei dati non-personali, è destinato a rimanere deluso. Secondo una logica lapalissiano, il testo di quest'atto si limita a dire infatti che sono "non-personali" «*i dati diversi dai dati personali*» (art. 2), optando così per una definizione che confermerebbe il centralismo RGPD.

### *2.3. Il concetto di dato personale, da small a big data*

Dalla ricognizione dell'attuale statuto giuridico dei dati emerge un scenario alquanto incerto, all'interno del quale, però, il concetto di dato personale gioca un ruolo di primo piano. Come già ricordato, si tratta di una nozione che nel tempo ha conosciuto diverse evoluzioni, rispetto alle quali il Gruppo di lavoro Articolo 29 (WP29)[540] e la CGUE negli anni hanno svolto un ruolo chiave, contribuendo a chiarirne di volta in volta la portata.

In un primo momento, la giurisprudenza si era limitata a chiarire come questo concetto comprendesse elementi apparentemente ovvi come – ad esempio – nomi, recapiti[541] e indirizzi[542]. In seguito, poi, soprattutto lo per lo stretto legame storico che unisce la protezione dei dati alla tutela della *privacy*, i giudici europei hanno cominciato a considerare anche profili più articolati, includendo varie proiezioni della vita professionale[543] o della situazione patrimoniale[544].

È stato però soprattutto con lo sviluppo dei nuovi *media*, delle tecnologie dell'informazione e del *web*, che questo concetto ha avuto bisogno di ulteriori e più approfondite specificazioni, cui ha provveduto dapprima il Gruppo Articolo 29, con un parere *ad hoc*[545] e, in seguito, la giurisprudenza di Lussemburgo.

---

[540] Si tratta di un Gruppo di lavoro indipendente previsto dall'art. 29, dir. CE 46/95 (da cui a poi preso il nome: Gruppo Articolo 29) deputato allo svolgimento di funzioni consultive. Con il nuovo regolamento quest'ente è stato sostituto dal Comitato europeo per la protezione dei dati personali, previsto *ex* art. 68, reg. UE 679/2016. In questa transizione, tuttavia, le linee guida e i pareri in precedenza emanati dal Gruppo Articolo 29 sono ritenuti validi finché non rivisti e riformati dal nuovo Comitato.

[541] Sentenza *Linqvist*, § 24.

[542] Sentenza *Rijkeboer*, § 42.

[543] Sentenza *Linqvist*, *ibidem* (i passatempi); sentenza *Worten* §§ 19 e 22 (i periodi di lavoro e di riposo).

[544] Sentenza *Österreichischer Rundfunk e a.* § 64 (gli stipendi); sentenza *Satakunnan Maskkinapörssi e Satamedia* §§ 35 e 37 (il patrimonio o altre forme di reddito).

[545] Gruppo Articolo 29, *Parere 4/2007 sul concetto di dato personale,* 20 giugno 1007, WP136 (disponibile a questo link, visitato il 5.12.2018, in seguito solo WP136).

In primo luogo, si è tornati a sottolineare con enfasi come il concetto di dato personale sia una nozione volutamente ampia[546], orientata a garantire un elevato livello di protezione dei diritti soprattutto per quel che riguarda lo sviluppo di tecnologie nuove. A prescindere dal formato con cui i contenuti possano essere raccolti, trattati o conservati, questa si presta perciò ad includere tutte le *affermazioni*[547] riferibili ad uno specifico individuo. Il fatto che le informazioni siano idonee a identificare il soggetto, dunque, non sarebbe l'unico elemento dirimente poiché, per ritenere personale un contenuto, rileverebbe soprattutto la sua capacità di incidere sulla sua sfera giuridica dell'individuo, estendendo così la portata della definizione ad una vasta gamma di trattamenti.

Per questi motivi, nell'interpretare la nozione di dato personale è necessario concentrare l'attenzione anche – e soprattutto – sulle finalità e sulle conseguenze dell'utilizzo dei dati. Anche in mancanza dei comuni «elementi di "contenuto" o di "finalità", – infatti – è possibile considerare che i dati "concernono" una persona quando il loro impiego può avere un impatto sui diritti»[548]. In tal senso, dunque, non sarebbe necessario «che il risultato potenziale abbia un impatto importante. [Ma è] sufficiente che la persona sia trattata in modo diverso rispetto ad altre in seguito al trattamento di tali dati»[549].

Considerando queste indicazioni, la Corte di giustizia ha quindi esteso ulteriormente la portata del concetto in esame, tanto da ricondurre nell'alveo di questa disciplina anche informazioni che inizialmente sembravano doversi escludere[550].

---

546 *Ibidem, 6*

547 *Ibidem,* 10-11

548 *Ibidem*, 11.

549 *Ibidem.*

550 Emblematici in questo senso, sono gli *overruling* registrati in occasione delle sentenze *Breyer* (rispetto a quanto in precedenza deciso nella sentenza del 24 novembre 2011, *Scarlet Extended* (C-70/10)) e sentenza *Nowak* (rispetto, invece, a quanto deciso con la sentenza del 17 luglio 2014, *YS e a.* (C-141/12 e C-372/12)) che si andranno ad analizzare nel prossimo paragrafo.

Per capire la portata di queste affermazioni, basta prendere in esame anche alcune sentenze recenti, da cui si possono facilmente evincere gli argomenti che stanno alla base di questi ormai consolidati orientamenti. Nel caso *Nowak*[551]– ad esempio – si trattava di decidere se le prove di un esame scritto (e le relative correzioni) potessero essere ricondotte al concetto di dato personale, consentendo così al candidato (soggetto interessato) di prendere visione dei suoi elaborati esercitando il suo diritto di accesso[552].

Con questo *escamotage*, evidentemente, si è tentato di ottenere con l'accesso ai dati personali quello che in alcuni ordinamenti si può conseguire con l'accesso agli atti amministrativi (com'è previsto anche, in specie, dal diritto italiano). Comparando rapidamente la *ratio* di queste due prerogative, peraltro, sembrerebbe che la prima intenda limitarsi alla possibilità di ottenere la disponibilità delle informazioni, mentre la seconda possa invece consentire di conoscere le motivazioni di una certa decisione[553].

Per questi motivi, nella sua precedente giurisprudenza, la Corte si era dimostrata restia nel ricondurre alla nozione di dato personale valutazioni e motivazioni relative alla condizione del soggetto interessato[554]. Sebbene, queste possano contenere o fondarsi su questo tipo di informazioni, si era infatti preferito mantenere i due concetti distinti[555].

Contrariamente a questo orientamento, tuttavia, nel caso *Nowak* i giudici europei si sono determinati per una soluzione di segno opposto. Capovolgendo i termini della questione, si è osservato come gli esiti delle prove siano di per sé idonei ad incidere sulla sfera giuridica dell'interessato, influenzandone anche le scelte relative alla vita privata. Per tale motivo, dunque, è sembrato ragionevole estendere

---

551 Sentenza del 20 dicembre 2017, *Nowak* (C-434/16).
552 Art. 12, lett. a) e b), dir. CE 95/46.
553 Una constatazione peraltro emersa chiaramente nelle conclusioni dell'AG in *YS e a.*
554 Sentenza *YS e a.*
555 *Ibidem*.

la nozione di dato personale anche a questi contenuti, così da garantire al candidato l'esercizio del diritto di accesso e degli altri rimedi giuridici cui questo è preordinato.

Alla luce di questa breve disamina, dunque, si può osservare come la plasticità della definizione di dato personale sia stata utilizzate per includere all'interno di questa materia la tutela di situazioni nuove, estendendo il concetto di informazione personale anche a contenuti che non sarebbero immediatamente riconducibili al senso classico della definizione.

La giurisprudenza recente, peraltro, ha offerto altre occasioni per riflettere anche sulle questioni legate all'ambiguo rapporto semantico tra dati e informazioni e così sulle questioni che possono emergere nel trattamento dei dati pseudonimizzati o anonimi.

Ciò si evince – ad esempio – in quanto deciso nel caso *Breyer*[556]. All'origine della questione si era posto il dubbio se gli indirizzi IP dinamici dovessero rientrare o meno nel perimetro della definizione di dato personale[557]. In merito, da un punto di vista tecnico, si tratta di identificativi che non individuano le persone, bensì le macchine, ovvero i dispositivi di cui l'utente si avvale. Quando uno di questi sistemi si connette alla rete[558], il gestore del servizio registra il numero che lo identifica (c.d. IP statico) e, nell'indirizzare l'utente alla pagina richiesta, genera un nuovo codice (c.d. IP dinamico) che trasmette al fornitore dei contenuti. Di questi due *providers*, solo il primo dispone delle informazioni necessarie ad identificare il *device* e così, indirettamente, si presume sia in grado di individuare anche l'utente che lo utilizza. Vista la posizione dei titolari del trattamento, nel qualificare queste due stringhe, inizialmente la prima – l'IP statico[559] – era già stato incluso nel perimetro della disciplina sui dati personali, la seconda invece no.

---

[556] Sentenza del 19 ottobre 2016, *Breyer* (C-582/14).
[557] Dir. CE 95/46, art. 2, lett. a.
[558] *Ibidem*, § 16.
[559] *Ibidem*, § 25. Cfr. Sentenza del 24 novembre 2011, *Scarlet Extended* (C-70/10), § 51.

A prima vista si tratterebbe di un tipico caso in cui la personalità dell'informazione risulta essere in parte mitigata, proprio perché il fornitore dei contenuti di per sé dispone di informazioni che non gli consentono di identificare l'utente (quanto meno non direttamente). La Corte di giustizia, tuttavia, in quest'occasione, ha deciso di includere ugualmente questo tipo di identificativi nella nozione di dato personale, osservando che il destinatario degli IP dinamici potrebbe comunque ottenere i dati che gli servono a conoscere i suoi visitatori[560], avvalendosi eventualmente dell'aiuto di terzi. Questi codici, pertanto, oggi rientrano a tutti gli effetti nella categoria dei dati personali e questo non tanto per l'effettiva natura del dato in sé considerato, quanto in ragione delle dinamiche relative al suo trattamento, anche nei rapporti tra diversi titolari[561].

Ricapitolando, dunque, in linea con gli orientamenti dell'GEPD, entrambe queste pronunce estendono il concetto di dato personale ad ogni contenuto che possa avere un impatto sulla sfera giuridica del soggetto, mentre il fatto che il dato *a priori* abbia una qualche chiara correlazione con il soggetto interessato sembra passare in secondo piano.

### *2.4. La protezione dei dati personali come diritto passe-partout?*

Com'è noto, la Corte di giustizia negli ultimi anni si è contraddistinta per aver avuto un ruolo particolarmente attivo sulla tutela dei diritti in dimensione digitale e la scelta di questo approccio garantista le è valso elogi e critiche.

In tal senso, si può osservare come, se la tutela dei diritti nella società dell'informazione sembra dipendere dal carattere personale delle informazioni, si corre il rischio di ricondurre a questo concetto anche situazioni che potrebbero

[560] eventualmente con l'ausilio di soggetti terzi *Ibidem*, §§ 47-48.
[561] *Ibidem*, §49 e § 64.

trovare soddisfazione altrimenti. Non di rado, i giudici europei per assicurare le necessarie tutele sembrano disposti a "riplasmare" l'ambito di applicazione della disciplina, focalizzandosi più sul risultato che una certa interpretazione permette di ottenere, che non sull'effettiva portata della definizione.

In una prospettiva di breve periodo, si avverte come questo tipo di interpretazione del concetto di "dato personale" possa rendere particolarmente difficile l'applicazione di questa disciplina. Chi si trova a dover trattare con i dati – soprattutto con dati apparentemente non-personali – spesso può avere seri dubbi sulla natura delle informazioni che utilizza e il disallineamento tra definizioni tecniche e giuridiche contribuisce a incrementare queste incertezze.

Lette pensando ai problemi che emergono di fronte ai *big data*, all'Ai o all'IoT, questi precedenti sollevano peraltro perplessità ben maggiori. Nella prospettiva dell'interessato, certo, simili conclusioni rincuorano, in quanto sembrano escludere la possibilità che di diritti d'azione di quest'ultimo possano essere limitati a causa della scarsa personalità del dato. Da un punto di vista complessivo, però, l'esito di queste interpretazioni potrebbe portare ad includere nella nozione di dato personale praticamente ogni genere di informazione, facendo di questa disciplina una nuova *law of everything* molto difficile da applicare[562].

In prospettiva, dunque, c'è da chiedersi come questa disciplina possa effettivamente contribuire ad una migliore tutela dei diritti e dove, invece, sia necessario cominciare ad elaborare altre soluzioni complementari[563].

---

[562] Se per assurdo si arrivasse davvero ad una situazione di questo genere, si teme infatti che di fronte alla difficoltà di ottemperare in modo effettivo agli oneri imposti da questa normativa, alcuni operatori decidano di ripiegare su un'interpretazione formale del loro ruolo, anche a discapito della tutela dei diritti fondamentali degli interessati.

[563] N. PURTOVA, *The law of everything. Broad concept of personal data and future of EU data protection law,* cit.

### 3. Stato di diritto, *privacy* e *big data*

Chiarita la potenziale pervasività della disciplina sulla protezione dei dati personali rispetto all'utilizzo dei *big data* – e, più in generale, delle tecnologie *data-intensive* – si può quindi passare ad approfondire la portata delle competenze europee in questa materia e i margini di discrezionalità siano lasciati invece al legislatore nazionale.

Alla luce di quanto previsto dall'art. 16 TFUE, seguendo sempre la logica di un *case-study*, nelle prossime pagine si andrà ad esaminare il contributo di alcune sentenze alla definizione di questi rapporti tra diritto comunitario e diritto statale. In particolare, ci si concentrerà sugli ambiti in cui tradizionalmente è accordato un maggior grado di autonomia rispetto a quanto deciso a Bruxelles, soprattutto per le questioni che riguardano l'utilizzo dei dati personali nell'ambito sicurezza nazionale e per finalità di pubblico interesse[564].

L'obiettivo è quello di mettere in luce le linee di indirizzo attorno alle quali cominciano a definirsi i tratti di una *digital rule of law* europea, approfondendo in particolare i profili inerenti la forza espansiva della disciplina sulla protezione dei dati e così delle competenze europee in settori storicamente improntati a delle logiche interne.

[564] Materia, come si ricorderà, normalmente esclusa dalle competenze europee (art. 16, § 2, TFUE, ultimo periodo: « Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea») e dall'ambito di applicazione della relativa disciplina (reg. 679/2016, artt. 2 e 23).

### *3.1. Stato di diritto, protezione dei dati e dataveillance*

Uno dei temi che si incontrano affrontando le questioni legate alla protezione dei dati personali nell'ambito delle materie tradizionalmente rimesse al legislatore nazionale riguarda il rapporto tra *data protection* e *rule of law*.

Se si ricorda, la disciplina in questo campo era nata proprio per evitare indebite interferenze degli attori pubblici nella vita privata, soprattutto quando questa potesse in concreto tradursi in nuove forme di controllo informatizzato[565]. Ed è proprio in quest'ottica che si affermano alcuni principi essenziali di questa normativa: basti pensare ai presupposti di legalità e liceità del trattamento, alle limitazioni relative alla quantità di dati raccolti e alle finalità del loro utilizzo.

Non è avventata, dunque, l'affermazione secondo cui la protezione dei dati personali, per certi versi, si propone di garantire il rispetto delle garanzie dello Stato di diritto in una dimensione informatizzata, imponendo una serie di regole volte a tradurre dei principi "analogici" in chiave "digitale".

Per tali motivi, considerata la pregnanza di questo tipo di norme nel definire i rapporti tra i cittadini e lo Stato[566], l'elaborazione della disciplina in detti ambiti ha sempre trovato forti resistenze nei confronti del legislatore comunitario[567]. Non solo

---

[565] Si veda quanto ricordato nel capitolo 1, § 2.1.

[566] Basti pensare al ruolo cui sono chiamate le garanzie relative alla libertà personale, al diritto di difesa, alla privatezza della propria dimora, della corrispondenza e delle comunicazioni nelle diverse esperienze costituzionali; normalmente prima garanzia a favore del singolo rispetto ai poteri coercitivi e di controllo che lo Stato può utilizzare solo per fondati e comprovati motivi.

[567] Tra gli interventi di carattere generale, infatti, a seguito di quanto deciso nel Consiglio europeo di Tampere del 1999, si sono affermati una serie di interventi ispirati al principio della "disponibilità" alla circolazione delle informazioni aventi rilievo giudiziario o di polizia, con l'obiettivo di promuovere nuove forme di *data sharing* tra le autorità di c.d. *law enforcement*. Sulla base di queste premesse, il principio di disponibilità ha trovato spazio per la prima volta nel Programma dell'Aja del 2004 e, in seguito, nella decisione 2006/969/GAI, destinata alle forze di polizia. Questo processo, in seguito, è continuano attraverso il c.d. *Prüm Process*, attraverso gli input politici stabiliti dal Trattato di Prüm. Cfr. R. BELLANOVA, *The "Prüm Process", the Way Forward for EU Police Cooperation and data exchance?* in E. GUILD, F. GEYER (a cura di), *Security versus justice? Police and Judicial Cooperation in the European Union*, Farnham, 2008.

inizialmente si è discusso se fosse opportuno regolamentare a livello europeo la normativa sull'utilizzo dei dati nel settore pubblico[568] ma, nel tempo, la disciplina sulla protezione dei dati personali nell'ambito della cooperazione penale continua ad essere un punto di confronto aperto[569]. Si tratta infatti di aree particolarmente delicate per la politica interna degli Stati membri, rispetto alle quali si scontrano sensibilità e culture tra loro assai diverse. Se cioè in alcuni Paesi possono risultare cruciali le questioni legate ai limiti legali al trattamento dei dati personali – secondo una sensibilità orientata alla massima tutela della libertà personale – in altri ordinamenti i problemi emergono non tanto rispetto al fatto che possano essere raccolti e conservati alcuni dati, quanto rispetto alle possibilità di un loro riutilizzo per altre finalità.

Alla luce di queste considerazioni, dunque, sono ben intuibili i motivi per cui in tali ambiti si sono frapposti vari ostacoli all'ipotesi di adottare un'unica normativa comune; tant'è che il trattamento dei dati personali in materia penale, soprattutto per quel che riguarda la sicurezza nazionale e l'ordine pubblico, rimane fortemente ancorata a delle logiche interne[570].

Questo stato di cose, tuttavia, dopo gli attentanti dell'11 settembre 2001, è stato messo fortemente in discussione. Se già in precedenza si sono registrati innumerevoli tentativi per potenziare la cooperazione internazionale in materia penale e a di polizia, il dilagare di questo tipo di attività criminose a livello internazionale (peraltro a danno di Europa e Stati Uniti) ha incoraggiato ad adottare misure decisamente più incisive. Non solo si sono potenziati i sistemi di coordinamento e collaborazione, favorendo l'adozione di politiche comuni ma, soprattutto a livello nazionale, si sono adottate varie strategie di contrasto e

---

568 In merito, si rinvia a quanto già accennato nel capitolo 3, § 1.2.

569 Basti pensare al fatto che anche le recenti direttive

570 Gli atti di coordinamento nel tempo intervenuti a livello comunitario hanno sempre lasciato un ampio margine di discrezionalità al legislatore nazionale, rimanendo fortemente ancorati al confronto intergovernativo, come dimostrano…

prevenzione, intensificando i controlli ad ampio spettro così da poter evitare i futuri attacchi[571].

Nell'ambito di queste politiche, l'utilizzo dei dati ha svolto un ruolo di primo piano. Considerando infatti le diverse fonti da cui oggi si possono attingere informazioni relative alle persone, alle loro abitudini, ai loro *networks*, si è cominciato a cogliere appieno il potenziale di questi nuovi strumenti di controllo. Nei più diversi ambiti[572] sono stati così istituiti dei sistemi di monitoraggio basati sullo sfruttamento intensivo di grandi quantità di informazioni raccolte. Tuttavia, la porta di queste iniziative è stata tale da aver determinato l'emergere di una sorta di nuovo fenomeno, prontamente identificato con il termine *dataveillance*[573]: degli innovativi sistemi di sorveglianza fondati, per l'appunto, sul controllo dei dati.

Chiaramente simili prassi si pongono in aperta antitesi con i principi sulla protezione dei dati personali, determinando peraltro pesanti ingerenze sulle libertà e diritti degli individui, primo tra tutti il diritto alla *privacy*. Cionondimeno, a fronte della minaccia incombente e dei rischi legati a questo tipo di criminalità organizzata, si è ritenuto che la situazione fosse tale da giustificare il ricorso a misure e poteri emergenziali [574] . Per assicurare l'incolumità delle persone e l'integrità dell'ordinamento, in molti Stati sono quindi state poste in deroga le tradizionali

---

[571] M. TZANOU, *The Fundamental Right to Data Protection*, cit.

[572] Come emerge chiaramente dall'analisi proposta in M. TZANOU, *The Fundamental Right to Data Protection. Normative Value in the Context of Counter-Terrorism Surveillance*, cit., oltre alla conservazione dei metadati, le strategie di contrasto hanno incluso anche la conservazione e l'accesso ai dati PNR e ai registri passeggeri, i dati finanziari e i dati relativi alla navigazione su internet.

[573] C. RAAB, D. WRIGHT, *Surveillance: Extending the Limits of Privacy Impact Assessment*, in D. WRIGHT, P. DE HERT (a cura di), *Privacy Impact Assessment*, Cham-Heidelberg-New York-Dordrecht-Londra, Springer, 2012, pp. 372 ss. riprendendo un concetto in precedenza elaborato a partire dal 1997 da R. CLARKE, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, disponibile al sito: http://www.rogerclarke.com/DV/Intro.html.

[574] Sul punto si vedano le considerazioni espresse in G. DE MINICO, *Costituzione. Emergenza e terrorismo*, cit.; DE VERGOTTINI, *Guerra e Costituzione. Nuovi conflitti e sfide alla democrazia*, cit.; A. VEDASCHI, *À la guerre comme à a la guerre? La disciplina della guerra nel diritto costituzionale comparato*, Torino, Giappichelli, 2007, pp. 75 ss. e 504 ss.

garanzie della *rule of law*, per orientarsi verso nuove *policy* pensate per venire incontro alle esigenze del c.d. «terrorismo del tempo ordinario»[575].

La situazione appena descritta, a livello europeo, ha offerto l'occasione per dare un forte impulso allo sviluppo di nuove politiche comuni, incoraggiando l'adozione di azioni condivise in ambiti in cui storicamente c'era stato un margine di manovra assai ridotto[576]. Guardando però alle competenze in materia di protezione dei dati personali, si osserva come la cooperazione in materia penale e di polizia costituisca un ambito in cui si fatica a trovare punti di accordo condivisi (quanto meno con il metodo comunitario). Sebbene attorno ai dati personali in questi settori gravitino una pluralità di interessi (spesso coinvolgendo anche gli attori privati e i fornitori dei servizi, e così i loro prerogative economiche) l'elemento centrale di queste politiche rimane fortemente ancorato al substrato costituzionale di ciascun ordinamento e, in particolare, al nucleo essenziale delle libertà personali.

In quest'ottica si spiegano dunque le questioni emerse attorno all'ormai annullata dir. 2004/26, nonché al valore "costituzionale" degli artt. 7 e 8 della Carta di Nizza e – soprattutto – dell'art. 16 TFUE.

Come già ricordato, sull'onda dei primi attentati europei di Madrid e Londra, dopo aver cassato una proposta di decisione quadro, ci si era orientati verso una direttiva ancorata al primo pilastro. Ragionando sull'uniformazione degli oneri imposti agli operatori privati, si erano definiti a livello europeo nuovi obblighi di conservazione dei metadati di traffico, rimettendo poi al legislatore nazionale la disciplina sulle condizioni di accesso, e così il bilanciamento tra interesse generale e diritti fondamentali.

---

[575] G. DE MINICO, *Le libertà fondamentali in tempo di ordinario terrorismo*, in *Federalismi.it*, 20 maggio 2015, p. 3.

[576] A. VEDASCHI, V. LUBELLO, *Data retention and its Implication for the Fundamental Right to Privacy*, cit., p. 18.; A. VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto. La "data retention" al test di legittimità*, cit.

La scelta così operata ha sollevato importanti critiche da parte di alcune Corti costituzionali nazionali, intese a sottoporre quest'indebolimento delle garanzie a favore della *privacy* ad un attento scrutinio di proporzionalità. Tali reazioni, così come le iniziative intraprese in seguito a livello europeo, meritano particolare attenzione, poiché costituiscono le linee guida sulle quali si sta andando ora sviluppare la futura strategia di *data governance* comunitaria. Affrontando un vero e proprio caso di legittimità costituzionale europea[577], la Corte ha infatti stabilito dei principi rispetto ai quali, nel tempo, sarà difficile tornare indietro. Così, comprenderne le premesse e i corollari risulta condizione essenziale per cogliere in prospettiva qual è e cos'è destinato ad essere il diritto alla protezione dei dati nei rapporti tra diritto nazionale e comunitario.

### *3.2. Le prime reazioni delle Corti costituzionali nazionali alla dir. 2006/24*

Ricostruendo l'evoluzione della lunga *querelle* giudiziaria che ha interessato la disciplina comunitaria sulla *data retention,* va osservato come, in un primo momento, il dibattito sulla dir. 2006/24 si è concentrato sulle questioni relative alla base giuridica, e così alle competenze comunitarie a legiferare su un tema del genere[578].

Interpellata sul punto, la Corte di giustizia inizialmente si è dimostrata restia a mettere in discussione la scelta fatta. Si era osservato, infatti, come, al di fuori di uno

---

[577] Conclusioni dell'AG Cruz Villalòn del 12 dicembre 2013, *Digital Rights Ireland* (causa C-293/12), § 1 (secondo il quale il caso ha offerto alla Corte «l'occasione di pronunciarsi sulle condizioni alle quali è *costituzionalmente possibile* per l'Unione europea prevedere una limitazione all'esercizio dei diritti fondamentali […] mediante una direttiva e i relativi provvedimenti nazionali di recepimento»).

[578] La direttiva, infatti, come ricordato, era stata ancorata alle competenze previste *ex* art. 95 TCE (oggi art. 114 TFUE) come misura di protezione e tutela del mercato e non invece come materia del terzo pilastro, sulla base degli artt. 31, n. 1, lett. *c*) e 34, n. 2, lett. *b*) TUE. Cfr. Capitolo 2, § 2.2., lett. *d*).

specifico discorso sui diritti[579], le misure adottate a livello europeo risultassero perfettamente compatibili con quanto deciso. Il fatto che i singoli Stati avessero adottato autonomamente diverse misure di prevenzione aveva imposto agli operatori privati importanti oneri economici, tanto che «le divergenze tra le varie normative nazionali adottate in materia di conservazione dei dati relativi alle comunicazioni elettroniche potevano avere un'incidenza diretta sul funzionamento del mercato interno e che era prevedibile che tale incidenza tendesse ad aggravarsi»[580]. Sulla base di simili presupposti, la scelta di un direttiva a tutela del mercato risultava perfettamente coerente. Trattandosi infatti di una sorta di competenza "inter-pilastro", secondo la Corte, l'equilibrio raggiunto sembrava soddisfacente. Il diritto europeo avrebbe inciso soltanto sugli obblighi di conservazione armonizzando così la disciplina rivolta ai fornitori dei servizi; il diritto nazionale avrebbe definito invece le condizioni relative all'accesso, e così il bilanciamento di interessi tra sicurezza e *privacy*[581].

Alla luce di questi primi riscontri, tuttavia, le censure legate alla tutela dei diritti non hanno accennato a venir meno. Se in alcuni Stati si è procrastinato il recepimento della direttiva (anche fino ad incorrere in una procedura di infrazione)[582], in altri la legittimità della disciplina è passata al vaglio delle Corti nazionali (con esiti per lo più negativi).

---

[579] CGUE, *Irlanda c. Parlamento europeo e Consiglio dell'Unione europea* (causa C-301/06), § 57. Osserva la Corte che «occorre anche precisare che il ricorso proposto dall'Irlanda verte unicamente sulla scelta del fondamento normativo e non già su un'eventuale violazione dei diritti fondamentali derivanti dalle ingerenze nell'esercizio del diritto al rispetto della vita privata, che la direttiva 2006/24 implica»; ragion per cui il sindacato, in quella prima occasione, era stato circoscritto solo e soltanto a questi motivi di censura.

[580] *Ibidem*, § 71.

[581] *Ibidem*, § 80.

[582] Cfr. nota n. 129. CGUE, sent. 26 novembre 2009, *Commissione/Grecia*, causa C-211/09; Sent. 26 novembre 2009, *Commissione/Irlanda*, causa C-202/09; sent. 4 febbraio 2010, *Commissione/Svezia*, causa C-185/09; sent. 29 luglio 2010, *Commissione/Austria*, causa C-189/2009. In particolare, inoltre, va ricordata un'ulteriore procedura che, in seguito, ha visto coinvolta nuovamente la Svezia, condannata al pagamento di una somma forfettaria di 3 milioni di euro (sent. 30 maggio 2013, *Commissione/Svezia*, causa C-270/2011).

Da più parti si era osservato come il fatto di imporre la conservazione di una così grande quantità di informazioni rappresentasse di per sé un rischio per i diritti degli interessati. Soprattutto nei Paesi più attenti a questi temi[583] si erano riscontrati una serie di problemi, legati essenzialmente alla necessità e alla proporzionalità di queste nuove misure di *data retention*[584].

Sebbene le questioni più spinose fossero legate alle condizioni di accesso ai dati – e quindi alla legislazione nazionale – l'incidenza della normativa europea era comunque evidente. Per primo, il Tribunale amministrativo supremo della Bulgaria[585], da un punto di vista pratico, aveva riscontrato come la direttiva contribuisse in modo importante alla creazione di questi *database*. Nonostante, infatti, la responsabilità circa la tutela dei diritti spettasse ai singoli Stati, la normativa europea creava di fatto le premesse materiali per ogni possibile violazioni, aprendo la strada non solo possibili abusi da parte delle forze dell'ordine ma anche da parte degli operatori medesimi[586]. Da un punto di vista teorico, invece, la Corte costituzionale romena[587] aveva messo in luce come la conservazione di *tutti* i dati di comunicazione dell'intera popolazione contribuisse in qualche modo a capovolgere

---

[583] Si tratta soprattutto degli Stati che negli anni avevano gradualmente riconosciuto la funzione costituzionale della protezione dei dati personali, come Germania, Ungheria e Portogallo.

[584] Per una panoramica su questi temi, si rinvia a M. TZANOU, *The Fundamental Right to Data Protection*, cit., pp. [72-81]; E. KOSTA, *The Way to Luxemburg: National Courts Decisions on the Compatibility of the Data Protection Directive with the Rights to Privacy and Data Protection*, cit., pp. [345-356]; M. DICOSOLA, *La* data retention directive *e il dialogo tra Corti costituzionali e Corte di Giustizia nel sistema multilivello europeo*, in *DirittiComparati.it*, 20 febbraio 2014, *passim*.

[585] Tribunale amministrativo supremo della Bulgaria, sent. 11 dicembre 2008, n. 13627 (testo originale disponibile a questo link; commentario disponibile in lingua inglese a questo link). Per una breve analisi della pronuncia si rinvia a M. TZANOU, *The Fundamental Right to Data Protection*, cit., pp. 74-75.

[586] La direttiva 2006/24 è stata definita infatti uno degli strumenti più invasivi mai adottati a livello europeo (Cfr. G. BUTTARELLI, *What Future for the Data Retention Directive*, Gruppo Articolo 29, come citato in M. TZANOU, *The Fundamental Right to Data Protection*, cit., p. 75, nota n. 69)

[587] Corte costituzionale romena, sent. 8 ottobre 2009, n. 1258 (testo originale disponibile a questo link; testo disponibile in lingua inglese a questo link (traduzione non ufficiale)). A commento, *ex multis*, si rinvia a C. MURPHY, *Romanian Constitutional Court, Decision No. 1258 of 8 October 2009*, in *Common Market Law Review*, 47/2010, pp. 933 ss.; M. TZANOU, *The Fundamental Right to Data Protection*, cit., pp. 76-77.

la presunzione di innocenza, trasformando *tutti* gli utenti in potenziali sospettati[588]. A ciò si aggiungevano poi i problemi riscontrati dalla *Bundesverfassungsgericht* tedesca[589] in merito agli obblighi di sicurezza previsti a livello europeo, da più parti considerati assolutamente inadeguati rispetto all'impatto sui diritti fondamentali delle misure imposte[590]. Si intuiva infatti come, sebbene tali misure non fossero di per sé incompatibili con i principi di un ordinamento democratico [591], la conservazioni di così tante informazioni sulle persone potesse comunque ingenerare in esse il sentore di essere continuamente osservate, finanche ad inibirle nell'esercizio dei propri diritti in diversi ambiti[592].

Nonostante quindi una certa deferenza da parte di alcuni Giudici per i criteri stabiliti a livello europeo [593] e per la discrezionalità esercitata dal legislatore nazionale [594], ovunque si sono riscontrati sinceri dubbi circa la necessità e

---

[588] Corte costituzionale romena, sent. 8 ottobre 2009, n. 1258, p. 9 del testo in lingua inglese. («The Constitutional Court underlines that the justified use, under the conditions regulated by law 298/2008, is not the one that in itself harms in an unacceptable way the exercise of the right to privacy or the freedom of expression, but rather the legal obligation with a continuous character, generally applicable, of data retention. This operation equally addresses all the law subjects, regardless of whether they have committed penal crimes or not or whether they are the subject of a penal investigation or not, *which is likely to overturn the presumption of innocence* and to transform *a priori* all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes» [corsivo aggiunto]).

[589] Corte costituzionale federale tedesca, sent. 2 marzo 2010, *Vorratsdatenspeicherung* (1 BvR 256/08) (testo originale disponibile a questo link; testo disponibile in lingua inglese a questo link). Per un commento si rinvia a K. DE VRIES, R. BELLANOVA, P. DE HERT, S. GUTWIRTH, *The German Constitutional Court judgment on data retention: Proportionality Overrides unlimited surveillance (Doesn't it?)*, in S. GUTWIRTH, Y. POULLET, P. DE HERT, R. LEENES (a cura di), *Computers, Privacy and Data Protection: an Element of Choice*, Dordrecht, Springer, 2011, pp. 3 ss.

[590] 1 BvR 256/08, §§ 220 ss. del testo in lingua inglese.

[591] *Ibidem*, § 183.

[592] *Ibidem*, § 212 («Particular weight also attaches to the storage of the telecommunications data because the storage itself and the intended use of the stored data are not directly noticed by the persons affected, but at the same time they include connections which are engaged in with an expectation of confidentiality. As a result of this, the storage of telecommunications traffic data without cause *is capable of creating a diffusely threatening feeling of being watched which can impair a free exercise of fundamental rights in many areas*» [corsivo aggiunto]).

[593] Corte suprema di Cipro, sent. 1 febbraio 2022 sui ricorsi nn. 65/2009, 78/2009, 82/2009, 15/2010, 22/2010 (testo originale disponibile a questo link)

[594] Corte cost., sent. 135/2002, *Considerato in diritto*, §§ 2.1 e 2.2. (Cfr. Capitolo 1, § 2.3).

l'adeguatezza di questo comune sistema di *data retention*. Anche nei successivi giudizi di legittimità costituzionale, infatti, sono state contestate soprattutto le ingerenze che tali misure possono comportare rispetto ai contenuti essenziali del diritto alla riservatezza e alla protezione dei dati personali, invocando così – seppur a livello nazionale – una più attenta ponderazione d'interessi.

### *3.3. La sentenza Digital Rights Ireland: rule of law e big data*

Alla luce delle conclusioni cui erano pervenute le Corti nazionali, la CGUE, interpellata sul punto in occasione del ricorso *Digital Rights Ireland*, ha colto l'occasione per chiarire i punti più problematici della disciplina europea.

La diversa sensibilità dimostrata rispetto al tema dei diritti è stata in parte imputata soprattutto al mutato assetto istituzionale *post* Trattato di Lisbona. Riconosciuto appieno il valore alla Carta di Nizza, i giudici europei sembrano guadagnare confidenza rispetto al valore costituzionale del *bill of rights* europeo[595], trovando così il coraggio di affrontare le fragilità della precedente giurisprudenza sulla competenza[596]. Da una serie di questioni di legittimità costituzionale nazionale si è passati quindi ad un problema di legittimità costituzionale europea, chiedendo

---

[595] G. DE BÚRCA, *After the EU Charter of Fundamental Rights: the Court of Justice as a human rights adjudicator*, in *Maastricht Journal of European and Comparative Law*, n. 2/2013, pp. [168-184].

[596] Riprendendo, infatti, le considerazioni svolte in precedenza – in occasione della sent. *Irlanda/Parlamento e Consiglio* – nel ricorso *Digital Rights Ireland* è stato proposto un ulteriore motivo sulla corretta individuazione della base giuridica. La Corte nella sua decisione, analizzando dapprima la questione alla luce degli artt. 7 e 8, non arriva a decidere del punto ma nelle Conclusioni dell'AG il problema viene affrontato in modo più compiuto: l'ingerenza della conservazione nella sfera della vita privata sarebbe stata sproporzionata per una misura volta alla sola tutela del mercato interno e, allo stesso tempo, l'unico presupposto che avrebbe permesso di confermare la legittimità della base giuridica non avrebbe potuto essere altro se non l'art. 95 CE (§ 102).

alla Corte UE di chiarire se e in che misura le istituzioni comunitarie possano limitare con i propri atti la portata dei diritti fondamentali previsti dalla Carta[597].

In quest'occasione, dunque, sebbene i giudici europei formalmente non arrivino a discostarsi dalla precedente decisione[598], facendo leva su questi nuovi elementi, si sono prodigati in un'attenta rivalutazione delle questioni in esame.

Chiarito lo stretto rapporto che legava la dir. 2004/26 a quanto previsto soprattutto dagli artt. 7 e 8 della Carta[599], la Corte si premura di chiarire innanzitutto se gli obblighi previsti da questa normativa determinino una qualche ingerenza circa i diritti al rispetto della vita privata e alla protezione dei dati personali.

In tal senso, la direttiva in questione aveva imposto la conservazione di una considerevole quantità di contenuti[600], ponendo in deroga le normali garanzie previste dalle dir. 95/46 e 2002/58[601]. Rispetto a tale scelta, in un primo tempo, si era abbracciato un approccio dualista, rispetto al quale conservazione e accesso erano considerati due trattamenti e due discipline distinte: l'uno, in capo agli operatori privati onerati *ex lege* di queste incombenze (e quindi disciplinato dal diritto europeo); l'altro, in capo alle autorità di pubblica sicurezza nell'ambito delle loro

---

[597] L'AG, infatti, introducendo le proprie conclusioni, esordisce sottolineando come i due ricorsi offrano alla Corte «le offre l'occasione di pronunciarsi sulle condizioni alle quali è costituzionalmente possibile per l'Unione europea prevedere una limitazione all'esercizio dei diritti fondamentali nel senso particolare di cui all'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea» (§ 1). Un ruolo istituzionale – quello di giudice costituzionale – che in questi casi non solo viene implicitamente ammesso dalla CGUE ma che le viene riconosciuto anche dalle Corti nazionali che ad essa di sono rivolte, come sottolineato da A. VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto*, cit., 1241 e G. TIBERI, *Il caso* Tele2/Sverige/Watson, cit., 437.

[598] Anche alla luce di quanto esposto nella nota precedente, la Corte non arriva a riconsiderare il proprio orientamento sul punto della competenza comunitaria (§ 71), decide di analizzare la questione soltanto alla luce di quanto previsto dalla Carta.

[599] Invero, tanto nei ricorsi della sent. *Digital Rights Ireland* le doglianze erano state sollevate non solo con riferimento a questi due articoli ma anche e soprattutto richiamando i diritti tutelati dall'art. 11, in materia di libertà di espressione. Tuttavia, nonostante qualche accenno a quest'ultimo (specificamente v. § 28), secondo la logica della "maggiore esposizione" (A. VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto,* cit., 1235), l'indagine si è concentrata principalmente su queste due disposizioni, in tema di *privacy* e protezione dei dati personali.

[600] Dir. 2006/24, artt. 3, e 5, § 1.

[601] *Digital Rights Ireland*, sent. § 32.

attività in campo penale (di competenza del legislatore nazionale). Secondo tale impostazione, la tutela della riservatezza sarebbe dipesa soprattutto dalla disciplina sulle condizioni di accesso ai dati e quindi dalla discrezionalità esercitata dal legislatore nazionale nel bilanciare la tutela delle sfera privata con gli interessi di pubblica sicurezza.

Con il tempo, però, intuendo il potenziale dei *big data*[602], si è colto come oggi l'accesso rappresenti un'interferenza ulteriore e successiva rispetto alla mera conservazione dei dati[603]. Senza contare i rischi legati ad eventuali accessi *contra legem*[604], la dir. 2004/26, infatti, includeva nel perimetro di queste misure praticamente tutta la popolazione europea dotata di un'utenza[605]; una circostanza tale da ingenerare nelle persone «la sensazione che la loro vita privata [fosse] oggetto di costante sorveglianza»[606] per la mera disponibilità dei dati sul proprio conto.

Una simile situazione aveva sollevato un certo allarmismo, sollecitando un attento scrutinio circa la necessarietà e la proporzionalità degli obblighi imposti.

Chiarito come le ingerenze generate dalle disposizioni della direttiva non intaccassero il contenuto essenziale dei diritti al rispetto della vita privata e alla protezione dei dati personali[607], la Corte ha constatato come tale ingerenza rispondesse ad un obiettivo di interesse generale, ossia la lotta alla criminalità più grave e l'incolumità della sicurezza pubblica[608].

Considerata però la portata delle misure proposte e il loro potenziale intrusivo, pur avendo appurato l'oggettiva utilità della *data retention*, le ingerenze rispetto ai

---

602 A. SPINA, *Risk Regulation of Big Data: Has the Time Arrived for a Paradigm Shift in EU Data Protection Law?*, in *European Journal of Risk Regulation*, n. 2/2014, pp. [248-252], spec. p. 251.

603 *Digital Rights Ireland*, Sent., §§ 60-62.

604 *Digital Rights Ireland*, Sent., § 66. Cfr. A. VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto,* cit., pp. 1230-1231.

605 Dir. 2006/24, art. 5. *Digital Rights Ireland*, Sentenza, §§ 56-57.

606 *Digital Rights Ireland*, sent. § 37.

607 *Digital Rights Ireland*, sent., §§ 39-40.

608 *Ibidem*, § 41.

diritti in questione avrebbero dovuto limitarsi allo stretto necessario[609]. La normativa in esame, dunque, secondo i criteri sanciti dall'art. 52, § 1 CDFUE, in primo luogo avrebbe dovuto prevedere regole chiare e precise, disciplinando la portata e l'applicazione della misura *de qua* e imponendo dei «requisiti minimi» e delle «garanzie sufficienti» a tutela degli interessati[610].

In tal senso, ragionando sui criteri di competenza, il paradosso cui aveva condotto la scelta del fondamento giuridico era ormai evidente. Incardinando la disciplina nell'ambito del primo pilastro, la direttiva aveva finito per regolare soprattutto i profili inerenti la tutela del mercato, evitando di limitare ulteriormente l'autonomia nazionale in materia penale. A motivo di questa decisione, però, la struttura dell'articolato risultava precaria, soprattutto sul fronte della tutela dei diritti[611]. Comprensibilmente, a riguardo, non si potevano pretendere prescrizioni puntuali e dettagliate, poiché, così facendo, si sarebbe finiti per invadere le già menzionate competenze penali. Tuttavia, la mancanza alcune «garanzie minime»[612] finiva col creare ancora più problemi: lasciando un così ampio margine di discrezionalità al legislatore nazionale si rischiava di ottenere un recepimento deficitario rispetto ai canoni previsti dalla Carta[613]; e anche quando la disciplina statale avesse privilegiato un approccio garantista, questo non avrebbe comunque

---

609 *Ibidem*, §§ 51-52.

610 *Ibidem*, § 54.

611 A. VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto,* cit., 1229-1232; F. BIGNAMI, *Protecting Privacy Against the Police in the European Union: The Data Retention Directive*, cit., 113 ss.

612 *Digital Rights Ireland*, Conclusioni, § 125; Sentenza, § 54 e 65.

613 *Ibidem*, § 62. La direttiva non aveva neppure previso un obbligo previso degli Stati membri volto a stabilire alcune limitazioni minime circa l'utilizzo dei metadati. Come si avrà modo di constatare nell'analisi svolta sulla portata delle normative nazionali nel caso *Tele2 Sverige*, spesso queste si erano determinate ad includere nel novero dei reati presupposto fattispecie di minor gravità, estendendo dunque le ingerenze nei diritti *ex* artt. 7 e 8 ben oltre i fini originariamente previsti dalla Dir. 2002/58 (*Tele2 Sverige*, Conclusioni, § 230).

potuto compensare le effettive carenze della disciplina comunitaria, oggettivamente incompatibile con il *bill of rights* europeo[614].

Si è giunti così a concludere che – in quanto prescrittiva di specifiche limitazioni – la direttiva avrebbe dovuto avere un'elaborazione coerente anche sotto il profilo delle tutele. Nell'*ecologia* dell'atto, cioè, avrebbero dovuto trovare spazio anche alcuni riferimenti oggettivi alla sicurezza dei dati, in modo tale da assicurare un effettivo controllo sulle condizioni preordinate alla conservazione e all'accesso[615].

In tal senso, la disciplina avrebbe dovuto contenere (almeno per principi) criteri chiari e oggettivi, definendo il tipo di reati per cui sono ammissibili queste misure (e le eventuali deroghe per le comunicazioni sottoposte a segreto professionale); le condizioni sostanziali e procedurali minime per l'accesso; il numero e la qualifica dei soggetti che possono disporre dell'autorizzazione di accesso (e l'effettiva del controllo giurisdizionale su tali atti); nonché adeguati limiti di durata alla conservazione dei dati e ogni altra necessaria garanzia funzionale ad assicurare la protezione di tali contenuti.

Al contrario, il testo si limitava a prevedere che le normative nazionali avrebbero dovuto «rispettare pienamente i diritti fondamentali che risultano dalle tradizioni costituzionali comuni degli Stati membri e che sono garantiti dalla CEDU»[616], richiamando solo genericamente i contenuti delle direttive 96/45 e 2002/58[617].

Quanto alle lacune della normativa, dunque, *in primis*, si è osservato come non fosse stato previsto alcunché circa l'opportunità di prestabilire e limitare l'utilizzo di questi strumenti solo a determinati soggetti[618], mancando così di individuare in

---

614 *Digital Rights Ireland*, Conclusioni, § 126-131; Sentenza, § 58-68.
615 *Digital Rights Ireland,* Sentenza, § 61.
616 Dir. 2006/24, *Considerando* n. 25.
617 Dir. 2006/24, art. 7.
618 *Digital Rights Ireland*, Sentenza, § 62.

modo chiaro le autorità potenzialmente abilitate a ricorrervi[619]. In secondo luogo, si è notato come non fossero stati nemmeno contemplati dei limiti all'ulteriore utilizzo dei dati ottenuti[620], ammettendo così indirettamente che, una volta disponibili, gli stessi potessero finire per soddisfare fini diversi da quelli per cui erano stati conservati. Infine, quanto all'osservanza dei più elementari meccanismi di *checks and balances,* si era tralasciato il fatto che l'accesso avrebbe dovuto essere subordinato all'autorizzazione di un giudice o di una autorità indipendente[621]. La Corte, dunque, ha incoraggiato un ritorno a forme di controllo effettivo, onde evitare che l'affermarsi delle autocertificazioni potesse tradursi in un opaco autoreferenzialismo degli inquirenti[622], riaffermando quindi la centralità del principio di legalità e della riserva di giurisdizione anche per queste misure.

In definitiva, dunque, a fronte del sacrificio richiesto, indicazioni così vaghe sembravano confermare anziché smentire la fragilità del sistema, tanto da lasciare aperta la domanda su quali avrebbero dovuto essere, in concreto, le procedure per poter ottenere l'accesso ai dati in modo legittimo. La sentenza *Digital Rights,* rilevando queste ed altre lacune, è giunta pertanto a dichiarare l'invalidità dell'intera direttiva, individuando (seppur indirettamente) dei principi di tutela comuni per le procedure inerenti la *data retention*.

---

[619] Commissione europea, relazione della Commissione al Consiglio e al Parlamento europeo, *Valutazioni dell'applicazione della Direttiva sulla conservazione dei dati (Direttiva 2006/24/CE),* cit., 10 ss.; COCQ - GALLI, *Comparative law paper on data retention regulation in sample of EU Member States*, 2013, 13ss.

[620] *Digital Rights Ireland*, Sentenza, § 61.

[621] *Digital Rights Ireland*, Sentenza, § 62.

[622] Commissione europea, *Valutazioni dell'applicazione della Direttiva sulla conservazione dei dati (Direttiva 2006/24/CE),* cit., 10 ss.; COCQ - GALLI, *Comparative law paper on data retention regulation in sample of EU Member States*, cit., 13ss.

Con quella prima vittoria si è cominciato a sperare che quanto stabilito in sede europea avrebbe presto trovato spazio a livello nazionale, affinando una maggior sensibilità per questa nuova *digital rule of law*[623].

### *3.4. Diritto comunitario e discipline nazionali verso una digital rule of law*

Per quanto appena detto, la sentenza *Digital Rights Ireland* rappresenta una vera e propria pietra miliare della giurisprudenza europea, in quanto, prima di allora, la Corte UE non era mai arrivata a dichiarare l'invalidità di un intero atto normativo perché in contrasto con la Carta di Nizza. È per questo motivo che, a seguito di questa e altre pronunce, è stato messo in luce in modo particolare il ruolo assunto da quest'istituzione nell'ambito del sistema "costituzionale" comunitario[624].

Con questa pronuncia, infatti, ancora una volta «i giudici europei hanno sperimentato la loro capacità di essere rigorosi nella tutela dei diritti su uno dei terreni più spinosi, dato che la gravità della situazione internazionale tende ad attutire la sensibilità verso i diritti dei sospetti terroristi e genera una maggiore propensione verso le esigenze della sicurezza piuttosto che verso quelle della giustizia e della libertà»[625].

Tuttavia, così facendo, sono emersi nuovi e ulteriori problemi, soprattutto nei rapporti tra diritto nazionale e diritto europeo: da un lato, infatti, risulta sempre più critica l'attuazione dei principi stabili in *Digital Rights Ireland*; dall'altro, si rivela problematica la definizione di un "confine" delle competenze tra gli Stati membri e l'Unione.

---

[623] L. ARENA, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?* in *Quaderni Costituzionali*, 2014; VON DANWITZ, *The Rule of Law in the Recent Jurisprudence of the ECJ*, in *Fordham ILJ*, 2014, pp. 1332-1333.

[624] G. DE BÚRCA, *After the EU Charter of Fundamental Rights: the Court of Justice as a human rights adjudicator*, cit.;

[625] M. CARTABIA, *L'ora dei diritti fondamentali in Europa*, in ID. (a cura di), *I diritti in azione*, cit., p. 13.

Invalidata la normativa europea, erano rimaste comunque in vigore le leggi statali che ne avevano dato attuazione, le quali molto spesso avevano ereditato – quando ancora non aggravato[626] – i vizi contestati alla normativa europea. Si trattava dunque di chiarire come e a che condizioni la legislazione nazionale avrebbe dovuto conformarsi ai principi elaborati dalla giurisprudenza comunitaria, delineando soprattutto in concreto i limiti al legittimo utilizzo delle misure in questione.

A tal proposito, se individuare le carenze procedurali poteva essere un'operazione agile, delineare dei confini perentori all'utilizzo della *data retention* ha richiesto qualche ulteriore riflessione. L'occasione per approfondire ulteriormente il tema è stato offerta dapprima con il ricorso *Tele2 Sverige*[627], un rinvio promosso rispettivamente da Svezia e Regno Unito nel verificare la conformità delle proprie normative nazionali ai nuovi parametri europei.

Con il venir meno della dir. 2006/24, il principale riferimento normativo sul piano del diritto comunitario, è tornato ad essere infatti l'art. 15 della direttiva 2002/58 (la già ricordata direttiva *e-privacy*). Tale norma, individuando di specifici motivi di interesse pubblico, accorda agli Stati membri la *facoltà* di *derogare* il regime generale, ammettendo la conservazione dei metadati solo per favorire la prevenzione e la repressione dei reati più gravi. Trattandosi però di una disciplina ancorata anch'essa alle competenze di quello che era il "primo pilastro", il suo l'ambito di applicazione è circoscritto alle sole misure di tutela del mercato, escludendo così le materie che esulano dal campo di applicazione del diritto europeo e le attività riguardanti «la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di

---

[626] F. BIGNAMI, *Privacy and Law Enforcement in the European Union: the Data Retention Directive*, cit., 233; A. VEDASCHI, V. LUBELLO, *Data Retention and its Implications for the Fundamental Right to Privacy*, cit., 20; C. COCQ, F. GALLI, *Comparative law paper on data retention regulation in a sample of EU Member States*, cit., 11.

[627] CGUE, sent. 21 dicembre 2016, *Tele2 Sverige AB contro Post- och telestyrelsen e Secretary of State for the Home Department c. Tom Watson e a.* (cause riunite C-203/15 e C-698/15).

sicurezza dello Stato) o alle attività dello Stato in settori che rientrano nel diritto penale»[628].

Il primo punto da chiarire – interessante non solo per il caso in questione, ma in generale per le prospettive che esso apre circa la portata della normativa europea e delle competenze della Corte – ha riguardato l'ambito di applicazione della dir. 2002/58 e il rapporto che lega le deroghe *ex* art. 15, § 1 e le materie escluse *ex* art. 1, § 3.

Considerata la portata letterale delle singole norme, non vi è dubbio che la disciplina sull'accesso ai dati da parte delle forze dell'ordine rientri nelle prerogative degli Stati membri, trattandosi evidentemente di competenze «estranee ai settori di attività dei singoli» privati[629]. Tuttavia – osserva la Corte – alla luce dell'economia generale della direttiva in esame, la coincidenza tra le finalità che consentono di fruire del regime derogatorio e le materie escluse dall'art. 1, § 3, non consente di concludere che le misure adottate *ex* art. 15, § 1, della direttiva *e-privacy* siano totalmente escluse dall'ambito di applicazione di tale normativa onde evitare «di privare detta disposizione di qualsiasi effetto utile»[630]. Poiché dunque è la direttiva che autorizza espressamente gli Stati membri a dotarsi di nuove misure di *data retention*, tali misure sono da considerarsi legittime solo nella misura in cui rispettino i principi e le condizioni sanciti a livello europeo, dalla legislazione ordinaria e – ancor più – dalla Carta di Nizza.

I giudici europei, pertanto, analizzando la normativa *de residuo*, si sono resi conto che senza una pronta modifica delle discipline di attuazione, il regime istituito dalla dir. 2006/24 avrebbe continuato a coinvolgere un'enorme quantità di persone,

---

[628] Dir. 2002/58, art. 1, § 3.
[629] *Tele 2 Sverige*, sent. § 72.
[630] *Ibidem*, § 73.

tanto che quella che sarebbe dovuta tornare ad essere un'*eccezione* sarebbe comunque rimasta la *regola*[631].

Come suggerito dalla sentenza *Digital Rights Ireland*, il principio di proporzionalità richiederebbe innanzitutto che le ingerenze nei diritti fondamentali sanciti dall'artt. 7 e 8 CDFUE risultino commisurate alla gravità dei reati. L'obbligo di *data-collecting*, in questi casi, viene infatti prescritto in un momento in cui gli utenti interessati potrebbero non avere nulla a che fare con i fenomeni criminosi che si intende perseguire[632]; una ragione in più per cui si riteneva necessario procedere con particolare cautela. La previgente regolamentazione, aveva lasciato agli Stati una certa discrezionalità nell'individuare i reati presupposto, ammettendo la possibilità di un'interpretazione estensiva delle ipotesi inizialmente contemplate. Questa autonomia però era stata intesa in vari modi, tant'è che si è potuto osservare come la scelta di criteri differenti avesse finito con l'includere fattispecie assai diverse per natura e gravità[633].

---

. [631] Già nella sent. *Digital Rights Ireland*, si è osservato come, rispetto alla dir. 2006/24, l'«articolo 3, in combinato disposto con l'articolo 5, paragrafo 1, della stessa, la conservazione di tutti i dati relativi al traffico riguardante la telefonia fissa, la telefonia mobile, l'accesso a Internet, la posta elettronica su Internet nonché la telefonia via Internet. Pertanto, essa concerne tutti i mezzi di comunicazione elettronica il cui uso è estremamente diffuso e di importanza crescente nella vita quotidiana di ciascuno. Inoltre, conformemente all'articolo 3, la Direttiva riguarda tutti gli abbonati e gli utenti registrati. Essa implica pertanto un'ingerenza nei diritti fondamentali della quasi totalità della popolazione europea.» (§ 56). La pronuncia *Tele2 Sverige*, riprendendo il punto, ha dunque concluso che qualora la normativa nazionale, in accordo con le prescrizioni invalidate, fosse finita con il prevedere una conservazione generale e indifferenziata dei metadati, *«porta alla conseguenza che la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione costituisce la regola, quando invece il sistema istituito dalla Direttiva 2002/58 esige che tale conservazione dei dati sia l'eccezione» (*§ 104), violando il principio di necessità.

[632] G. DE MINICO, *Le libertà fondamentali in tempo di ordinario terrorismo*, cit., 4. L'Autrice sottolinea, infatti, come, in generale, l'utilizzo dei mezzi di contrasto al terrorismo chieda di mediare tra valori antagonisti in base alla proporzionalità di inveramento del rischio. Questo implica che la valutazione, dunque, consideri situazioni *disallineate in ragione del tempo*, *disomogenee nel sacrificio e nel vantaggio:* si nota come «infatti, il danno attuale e certo sopportato dal detentore del diritto alla riservatezza ha un peso maggiore del vantaggio procurato ai titolari del diritto alla sicurezza».

[633] Si rimanda inoltre alla relazione della Commissione al Consiglio e al Parlamento europeo, *Valutazioni dell'applicazione della Direttiva sulla conservazione dei dati (Direttiva 2006/24/CE)*, cit., 6 ss.; C. COCQ, F.GALLI, *Comparative law paper on data retention regulation in a sample of EU Member States*, cit., 11.

Alla luce dei principi di necessità e proporzionalità (questa volta approfonditi per l'individuazione di un vero e proprio limite[634]) la Corte ha dunque constatato che non tutti i crimini ammettono il ricorso a strumenti così intrusivi, che invece andrebbero limitati soltanto ai casi più gravi[635]. Con una sentenza "additiva"[636], il dettato dell'art. 15, § 1è così stato integrato, chiarendo che le ipotesi menzionate in tale norma sono da intendersi come esaustive[637]. La normativa sulla *data retention* risulta quindi compatibile con i criteri enunciati in *Digital Rights Ireland* soltanto nei caso in cui le misure siano finalizzate a perseguire reati di particolare gravità per «la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica»[638].

Alla luce di queste considerazioni, dunque, la Corte ha espresso un *favor* per misure più mirate, limitate ai soli casi in cui vi sia (o vi possa essere) una chiara relazione tra i dati raccolti e i soggetti interessanti, preferendo così alle misure generali rivolte all'intera popolazione, una serie di interventi "targettizzati"[639] e basati su fondati sospetti. Inoltre, in ossequio al principio di trasparenza, viene ribadita la doverosità dell'informativa nei confronti degli interessanti, così da assicurare *ex post* un effettivo esercizio del diritto al ricorso (senza che questo determini, chiaramente, un pregiudizio al risultato delle indagini)[640].

---

[634] O. POLLICINO, M. BASSINI, *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Diritto Penale Contemporaneo*, 2017, spec. 6-9.

[635] *Tele2 Sverige*, sent., § 115.

[636] TIBERI, *Il caso* Tele2 Sverige/Watson: *un'*iconica *sentenza della Corte di Giustizia nella saga sulla* data retention*,* in *Quaderni costituzionali*, 2017, 436.

[637] *Tele2 Sverige*, Sentenza, § 90 e 115.

[638] Dir. 2002/58, art. 15, § 1.

[639] G. FORMICI, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia* Ministerio Fiscal*,* in *Osservatorio Costituzionale*, n. 3/2018, p. 464.

[640] *Tele2 Sverige*, Sentenza, § 121.

La saga sulla *data retention* sembra così giungere ad un approdo in assoluta controtendenza con il generale clima securitario degli ultimi anni[641]. La Corte di giustizia, elaborando in via ermeneutica condizioni e limiti per queste misure, ha contribuito a normalizzarne l'utilizzo secondo le garanzie proprie dello Stato di diritto, ribaltando le precedenti posizioni di forza.

Da una dialogo cominciato su iniziativa della Corti nazionali, tese a far valere le proprie prerogative in materia di diritti fondamentali rispetto a quanto previsto dalla normativa europea, oggi si assiste ad una sorta di inversione di ruoli, in cui è la Corte di giustizia a dettare le condizioni di legittimità delle leggi nazionali[642].

Questo cambio di prospettiva, tuttavia, non è privo di conseguenze sul piano istituzionale, soprattutto se si pensa alle implicazioni pratiche del tema che qui ci occupa. I criteri elaborati dalla giurisprudenza europea, infatti, pur immediati nella loro portata valoriale, sono risultati particolarmente ostici nel recepimento, avendo mancato di chiarire i presupposti per una legittima conservazione dei dati, così come i parametri con cui definire la gravità dei reati che possono ammettere l'utilizzo della *data retention*. Per quanto si evince dalla sentenza *Tele2 Sverige*, è indispensabile sussista in tal senso un rapporto consequenziale tra la gravità del reato perseguito e la severità delle limitazioni imposte ai diritti fondamentali, tanto da ritenere implicitamente tassativa la lista di ipotesi contemplate all'art. 15, § 1, dir. 2002/58. Allo stesso tempo, però, la Corte non da ulteriori indicazioni circa il criterio di

---

641 O. POLLICINO, G.E. VIGEVANI, *Privacy digitale e conservazione dei dati di traffico per finalità di sicurezza: la sentenza* Tele2 Sverige *della Corte di giustizia UE*, in *Forum di Quaderni costituzionali*, 16 gennaio 2017.

Un orientamento peraltro confermato anche in occasione della sentenza *Schrems I* (CGUE, sent. 6 ottobre 2015, *Maximillian Schrems contro Data Protection Commissioner* (causa C-362/14)) e nel parere 1/15 (Accordo PNR EU-Canada) del 26 luglio 2017; altre due occasioni in cui la Corte, attingendo dai principi enucleati in occasione della pronuncia *Digital Rights Ireland*, ha fornito alcune indicazioni essenziali circa i criteri di validità degli atti della Commissione nei rapporti con gli Stati terzi.

642 F. GUELLA, Data retention *e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali*, in *Diritto pubblico comparato ed europeo – online*, 2/2017, pp. [349-357].

"gravità"[643], limitandosi a rifarsi genericamente ai fini di prevenzione, ricerca accertamento e perseguimento di attività criminali[644].

A seguito di queste pronunce, si sono quindi moltiplicati i rinvii volti a chiarire i rapporti tra quanto previsto disciplina statale rispetto a quanto prescritto a livello comunitario[645], offrendo così alla CGUE l'occasione per sviluppare ulteriormente la sua giurisprudenza "costituzionale" su questi temi[646].

A distanza di pochi anni, infatti, con il rinvio *Ministerio Fiscal,* i giudici europei hanno avuto un'ulteriore possibilità di tornare sul punto, ribandendo la propria competenza a decidere su queste materie e specificando ulteriormente la loro dottrina *rights oriented* rispetto ai «principi costituzionali dell'Unione»[647]. Sebbene il governo spagnolo si fosse rifatto alla storica impostazione dualista – ribadendo così come le richieste di accesso ai dati rientrino a pieno titolo nelle prerogative degli Stati all'esercizio dello *ius puniendi*[648] – la Corte ha infatti confermato che la deroga sancita dall'art. 15, § 1, dir. 2002/58 è invece in grado di attrarre nell'ambito di

---

643 Queste le considerazioni dell'AG Henrik Saugmandsgaard Øe nelle sue conclusioni del 3 maggio 2018, *Ministerio Fiscal* (causa C-207/16), in cui si legge: «sebbene detta sentenza [*Tele2 Sverige*] fornisse esempi di reati gravi, essa non definiva tuttavia in modo sufficientemente chiaro il contenuto sostanziale della nozione di gravità del reato che può servire da criterio di valutazione della giustificazione di una misura d'ingerenza. Orbene, tale nozione comporterebbe il rischio che le condizioni della conservazione dei dati e dell'accesso ai medesimi siano stabilite, a livello nazionale, in un modo molto ampio, che non rispetterebbe i diritti fondamentali di cui alla sentenza Tele2» (§ 27).

644 *Tele 2 Sverige/Watson*, sent. §§ [117-121].

645 CGUE, sent. 8 ottobre 2018, *Ministerio Fiscal* (causa C-207/16); domanda di pronuncia pregiudiziale proposta dall'*Investigatory Powers Tribunal*, Londra (Regno Unito) del 31 ottobre 2017, *Privacy International/Secretary of State for Foreign and Commonwealth Affairs* e a. (causa C-623/17); domanda di pronuncia pregiudiziale proposta dalla *Cour constitutionnelle* (Belgio) il 2 agosto 2018, – *Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX c. Conseil des ministres,* (causa C- 520/18).

646 Come osservato in dottrina, in queste operazioni, infatti, la Corte tende ricondurre le norme in materia entro «un "perimetro costituzionalmente" orientato o quanto meno *human rights oriented*»; O. POLLICINO, M. BASSINI, *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, cit., p. 4.

647 Domanda di pronuncia pregiudiziale proposta dall'*Audiencia provincial de Tarragona, Sección cuarta* (Spagna) il 14 aprile 2016, *Ministerio Fiscal* (causa C-207/16), § 2.

648 *Ministerio Fiscal,* sent. § 30.

applicazione di tale normativa anche la disciplina relativa alle attività delle autorità nazionali[649], tanto da ricomprendere nel campo di applicazione della stessa praticamente qualsiasi misura di *data retention* in materia penale[650]. Ciò sarebbe confermato, peraltro, dal fatto che tanto la conservazione quanto l'accesso presuppongono un'attività di trattamento riconducibile ai soggetti privati, i quali nel primo caso sono tenuti a non cancellare i contenuti e nel secondo a permetterne la fruibilità (un distinguo particolarmente critico nel era dei *big data*, in quanto la possibilità di tracciare un confine giuridico tra i dati personali trattati direttamente dagli autorità statali in ambito penale e quelli, invece, trattati dai soggetti privati per ragioni proprie e poi eventualmente riutilizzabili in altri ambiti per finalità di pubblico interesse, risulta un'impresa tutt'altro che facile).

Quanto al merito, invece, la Corte torna alla sua dottrina sui diritti fondamentali, partendo a ragionare non tanto dalla gravità dei reati quanto dalla severità delle limitazioni imposte alle prerogative sancite dalla Carta. Riprendendo gli spunti offerti in precedenza circa i principi di necessità e proporzionalità, torna a concentrarsi sulla natura dell'accesso, concludendo che nei casi in cui si tratti di quantità limitate di informazioni questo sia astrattamente ammissibile anche per reati di minor entità[651].

Come osservato dall'AG Saugmandsgaard Øe nelle sue conclusioni, simili soluzioni non sono prive di rischi sul piano dei rapporti istituzionali tra Unione e Stati membri. Sebbene la Corte abbia optato per una sentenza "tattica"[652], usando il discorso sui diritti per evitare di prendere posizione in modo diretto sui criteri per

---

[649] *Ibidem*, § 34.

[650] *Ibidem*, § 53: «per quanto riguarda l'obiettivo di prevenzione, ricerca, accertamento e perseguimento dei reati, occorre rilevare che la formulazione dell'articolo 15, paragrafo 1, primo periodo, della direttiva 2002/58 non limita tale obiettivo alla lotta contro i soli reati gravi, ma si riferisce ai «reati» in generale».

[651] *Ministerio Fiscal,* sent. § 57.

[652] G. FORMICI, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia* Ministerio Fiscal*,* cit., p. 467.

determinare la gravità dei reati in questione, il risultato non cambia. Pensando quindi alla portata espansiva dei principi stabiliti dalle pronunce *Digital Rights Ireland* e *Tele2 Sverige*, bisognerebbe comunque «evitare di adottare una concezione troppo ampia dei requisiti stabiliti dalla Corte in tali due sentenze, al fine di non ostacolare, in ogni caso non eccessivamente, la possibilità degli Stati membri di derogare al regime stabilito dalla direttiva 2002/58, ad essi concessa dall'articolo 15, paragrafo 1, di quest'ultima»[653], e queste per non correre il rischio di estendere oltre misura le competenze comunitarie anche in ambiti formalmente esclusi.

Guardando alle questioni pregiudiziali proposte alla Corte in seguito alle pronunce appena richiamate, si colgono dunque i potenziali conflitti che potrebbero aprirsi in futuro rispetto all'ambito di applicazione della disciplina comunitaria in questi settori. Se da un lato, infatti, ci si interroga sulla portata dei principi costituzionali europei rispetto alle attività di *intelligence*[654], dall'altro ci si chiede che tipo di bilanciamento suggeriranno i giudici lussemburghesi tra *privacy* e sicurezza, ora ribadendo come sia la stessa Carta di Nizza a fare di quest'ultima uno specifico diritto fondamentale, idealmente equiparato a tutti gli altri contenuti del *bill of rights* europeo[655].

La situazione, peraltro, non sembra destina a stabili evoluzioni, dal momento che anche la proposta per il nuovo regolamento *e-privacy* non prevede alcuna novità di rilievo circa il regime sulla *data retention*. Spetterà quindi alla Corte UE continuare a decidere i margini di autonomia di cui può godere il legislatore Statale a norma dell'art. 39 TUE, e questo – probabilmente – secondo i criteri di ampio respiro che, come si è visto, già ne hanno contraddistinto la giurisprudenza.

Sebbene ci si trovi di fronte ad un processo in divenire, sommando le considerazioni qui esposte con quelle presentate nel paragrafo precedente, si coglie

---

653 *Ministerio Fiscal,* conclusioni AG, § 90.
654 *Privacy International*, cit.
655 *Ordre des barreaux francophones et germanophone*, cit.

dunque tutto il potenziale espansivo della normativa europea sulla protezione dei dati. La Corte di giustizia si dimostra propensa ad una lettura di ampio respiro non solo nell'interpretazione dei presupposti materiali – estendendo così la nozione di dato personale ad una grande varietà di contenuti – ma anche nell'intendere la portata della disciplina comunitaria e così le proprie competenze nel decidere in materia. Se da un lato, quindi, si assiste ad una progressiva costituzionalizzazione della protezione dei dati personali come *digital rule of law*, non si può fare a meno di constatare come queste linee di indirizzo vengano progressivamente attratte in sede europea, anche pregiudicando le competenze (e, in qualche modo, le identità culturali) nazionali.

## 4. Diritti fondamentali, *big data* e valutazione del rischio

Sulla base di quanto detto nei paragrafi precedenti, a questo punto si può passare ad esaminare come la Corte di giustizia abbia utilizzato il parametro sancito dall'art. 8 CDFUE come diritto fondamentale.

Prima di procedere in quest'analisi, tuttavia, è utile soffermarsi sulla natura dei pregiudizi che possono derivare dall'utilizzo dei *big data*. A differenza dei trattamenti di dimensione ridotte, infatti, questi sistemi presentano rischi ben più elevati. Come infatti accade anche con altre tecnologie *data-intensive* (le varie forme di intelligenza artificiale, piuttosto che con l'Internet delle cose) processando un'incredibile quantità di informazioni in tempo reale, i programmi possono incorrere in diversi tipi di errori fino a proporre dei risultati distorti.

Per questo motivo, in linea con il principio di *accountability*, il nuovo regolamento ha promosso un approccio preventivo, volto ad anticipare la tutela fino alle prime fasi di progettazione.

Nonostante la bontà di questi tentativi, tuttavia, fintanto che non verrà a chiarirsi la funzione costituzionale della protezione dei dati personali e il rapporto tra questo e gli altri diritti fondamentali intercettati dalla datificazione, esiste un serio pericolo di incorrere in altrettante storture interpretative, anche alterando la gerarchia di valori definita dalle costituzioni nazionali.

Per far luce su questi aspetti, nel corso delle prossime pagine, si procederà quindi in quest'ordine. Una volta individuati i nuovi *data rights*, si passerà ad esaminare il ruolo delle valutazioni di impatto nello sviluppo delle tecnologie in esame. Sulla base di queste considerazioni, si andrà ad approfondire come i giudici europei oggi intendano il rapporto tra *data protection* e *privacy* e i problemi che ne possono derivare nei rapporti con il diritto degli Stati. Infine, si verificherà se e come il reg. 679/2016 consenta dei margini di apertura su questi fronti, anche alla luce della più recente giurisprudenza UE.

### *4.1. I big data come fattore condizionante l'esercizio dei diritti fondamentali*

Come ricordato[656], risulta molto difficile stabile in termini giuridici che cosa si intenda per *big data*. La definizione ricorrente del fenomeno tecnologico, tende a concentrarsi su elementi di scarso interesse sul piano del diritto, mettendo a fuoco soprattutto le componenti quantitative e qualitative legate al volume e alla varietà di informazioni disponibili e alla velocità con cui possono essere elaborate[657].

Le variabili appena accennate, tuttavia, risultano poco significative rispetto alle questioni che emergono circa la tutela della persona e dei suoi diritti, così come ai fini della protezione dei dati. In questa dimensione, infatti, importa non tanto delle

---

[656] Cfr. Introduzione, § 2.1.

[657] Il c.d. paradigma delle *3V*, ossia *Volume, Velocity* e *Variety*, inaugurato da Doug Laney all'inizio del 2000 (v. D. LANEY, *3D Management: Controlling Data Volume, Velocity and Variety,* MetaGroup (Gartner Data & Analytics), File 949, 6 febbraio 2001).

informazioni in sé e per sé, quanto che queste possano essere elaborate più e più volte attraverso algoritmi e *software* in grado di manipolare e accrescere il valore dei contenuti, producendo effetti sul singolo come su intere categorie di individui[658].

Date queste premesse, dunque, occorre tornare a riflettere ancora un momento sul potenziale di queste tecnologie all'atto pratico, così come alle conseguenze del loro utilizzo.

Il legislatore europeo si è dimostrato particolarmente attento a questo tema già all'epoca della dir. 95/46, quando, guardando alle criticità legate ai processi di decisione automatizzati, notava come, in questi casi, si corra il rischio di ridurre la persona alla sua «proiezione informativa» (*data-shadow*), oscurando la logica del procedimento dietro meccanismi opachi[659]. Tuttavia, con il rapido sviluppo di tecnologie incentrate sull'elaborazione dei dati personali, questo tipo di preoccupazioni risultano oggi esasperate, sollevando perplessità non tanto – e non solo – rispetto alla *privacy*, ma a tutta una serie di diritti fondamentali il cui esercizio oggi si esplicita in chiave digitale e algoritmica. Generando ogni istante un'incredibile quantità di informazioni, le persone e gli oggetti lasciano dietro di sé una lunga (e ricca) serie impronte "digitali", che aggregate ed elaborate permettono di studiare le attività, le interazioni e i comportamenti degli interessati, fino ad influenzarne le condotte, le idee e i sentimenti.

---

[658] D. BOLLIER, *The Promise and Perils of Big Data* Aspen Institute, Communications and Society program, 2010 (accessibile a questo link); A. MANTELERO, *From group privacy to collective privacy: towards a new dimension of privacy and data protection in the big data era*, in L. TAYLOR, B. VAN DER SLOOT, L. FLORIDI (a cura di), *Group Privacy: New Challenges of Data Technologies*, Cham, Springer, 2017, 145 ss.; A. MANTELERO, *La* privacy *all'epoca dei* Big Data*,* in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di)*, I dati personali nel diritto europeo*, cit., p. 1187.

[659] Cfr. COM(90) 314 final – SYN 287, 13.9.1990, p. 29. «The danger of the misuse of data processing in decision-making may become a major problem in future: the result produced by machine, using more and more sophisticated software, and even expert systems, had an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities». A commento, *ex multis,* si veda: L.A. BYGRAVE, *Automated profiling – Minding the machine: article 15 of EC Data Protection Directive and Automated Profiling*, in *Computer Law and Security Review*, 17, 2001, pp. 17 ss.

Queste considerazioni, certo, non sono estranee alla disciplina sulla protezione dei dati personali, sebbene non possano dirsi in essa esaurite e concluse. Soprattutto negli ultimi tempi, per quanto appena detto circa lo sviluppo delle tecnologie *data-intensive,* il tema ha quindi preso nuovo vigore, tanto che si comincia a ragionare di una nuova tipologia di diritti, identificabili come *data rights*: diritti legati all'utilizzo dei dati[660].

Gettando un ponte che ci ricolleghi con la precedente tradizione dei diritti fondamentali, analizzando i contenuti di questa recente categoria si possono distinguere sin d'ora due principali sottoinsiemi. Nel primo rientrano i c.d. *traditional data rights* ai quali vengono ricondotti i valori della *privacy*, la disciplina sulla protezione dei dati personali e la libertà di espressione; tutti quei diritti che storicamente sono legati al mondo dell'informazione e alla fruibilità dei suoi contenuti[661]. Nel secondo, invece, si collocano i c.d. *new data rights*, o meglio gli *altri* diritti fondamentali intercettati dall'utilizzo dei dati[662].

Se per quanto detto finora le implicazioni inerenti il primo dei due gruppi forse risultano più immediate, quelle relative al secondo qui meritano qualche

---

[660] Sebbene l'utilizzo del termine sia ormai ampiamente diffuso, il significato di questa locuzione è ancora controverso; tant'è che si prospettano diverse teorie. Se da un lato si parla di *data rights* con riferimento ai diritti *sui* dati, proponendo una visione concentrata soprattutto gli aspetti proprietari del problema (cfr. M. TISNE, *It's time for a Bill of Data Rights,* in *MIT Technology Review*, 14 dicembre 2018; disponibile a questo link), dall'altro si avanza invece l'ipotesi di una serie di diritti legati all'utilizzo e alla condivisione dei dati distillati attraverso la cultura dei diritti umani, secondo una logica di più ampio respiro (cfr. T.L. HARRIS, J.M. WYNDHAM, *Data Rights and Responsibilities: A Human Rights Perspective on Data Sharing*, in *Journal of Empirical Research on Human Research Ethics*, n.10/2015, pp. 334-337). La logica qui accolta è la seconda, soprattutto per come proposta e sviluppata in A. DALY, A. CARLON, T. VAN GEELEN, *Data and fundamental rights*, in V. MAK, E. TJONG TJIN TAI, A. BERLEE (a cura di), *Research Handbook in Data Science and Law*, Cheltenham-Nothampton, Edward Elgar Publishing, 2018, pp. 378-407.

[661] A. DALY, A. CARLON, T. VAN GEELEN, *Data and fundamental rights*, cit., pp. 381 ss.

[662] *Ibidem*, pp. 390 ss. Su questi punti si richiamano anche le riflessioni proposte dal Garante europeo sulla protezione dei dati personali in occasione del parere n. 8/2016 – *EDPS Opinion on coherent enforcement of fundamental rights in the age of big data,* parere del 23 settembre 2016, n. 8, pp. 5-6 e 8 – in cui, con riferimento alla Carta di Nizza, si analizzano le implicazioni relative non solo agli artt. 7 e 8 CDFUE (rispetto della vita privata e familiare e protezione dei dati personali) ma anche quelle inerenti il principio di non discriminazione (art. 21 CDFUE).

considerazione in più. Per far ciò, tuttavia, è necessario individuare chiaramente i criteri con cui possono essere individuate le singole aree di interesse, passando poi ad esaminare le incognite e i rischi più evidenti in ciascuna di esse.

Come intuibile, l'elemento che contribuisce ad includere nuovi diritti fondamentali nell'ambito dei *data rights* è il processo di datificazione in corso e, con esso, i complessi sistemi di algoritmi utilizzati da governi ed enti privati per dar senso a questa «inondazione informativa»[663]. In quella che è già definita una «società degli algoritmi» i parametri per la distribuzione di informazioni, possibilità e ricchezza sono implementati nel *design* dei sistemi di calcolo su cui lavorano programmi. Di conseguenza, per capire come dei *fundamental rights* possano accedere alla categoria dei *data rights* è necessario analizzare che tipo di conseguenze possono derivare dall'impego di questi strumenti nei diversi ambiti in vengono utilizzati.

In tal senso, nel tentativo di proporre una prima mappatura (necessariamente provvisoria e non esaustiva) gli interessi a venire in gioco sono quelli legati alla libertà di informazione e al pluralismo informativo. È bene fare attenzione come qui non ci si trovi davanti ad una semplice riproposizione degli storici contrasti tra *privacy* e libertà di espressione. In questo caso, infatti, il rapporto risulta essere di natura strumentale poiché dalle logiche con cui vengono elaborati i contenuti dipende il perimetro effettivo dei diritti in esame.

Come documentano alcuni studi, una crescente percentuale di persone, di prassi, si informa *online* e attraverso i c.d. nuovi *media*, rispetto ai quali i *social network* coprono una quota considerevole. Notoriamente il funzionamento di questi servizi è regolato da complessi sistemi di algoritmi che tendono a registrare e a tracciare le

---

663 Il Garante europeo, in tal senso, ha parlato di un «effetto segregazione», *EDPS Opinion on coherent enforcement of fundamental rights in the age of big data,* cit., p. 6. Sul punto si vendano anche, *ex multis,* E. PARISER, *Il filtro. Quello che internet ci nasconde*, Milano, Il Saggiatore, 2012; T. SHADMY, *The New Social Contract: Facebook's Community and Our Rights*, in *Boston International Law Review* 2019 (in corso di pubblicazione); K. KLONICK, *The New Governors: The People, Rules and Process Governing Online Speech*, in *Harvard La Review*, 2018, pp. 1599-1670; A. CHANDER, *Facebookistan*, 90 *North Carolina Law Review*, 2012, pp. 1808-1844.

preferenze degli utenti così da riproporre in seguito solo i contenuti che si ritiene possano essere di maggior interesse per ogni singolo fruitore. Così facendo, tuttavia, si ingenerano gravi effetti distorsivi, costruendo attraverso queste mediazioni delle «camere di risonanza» (*echo chambers*) entro cui ciascuno è esposto soltanto alle notizie che potrebbe voler ricevere.

Tutto ciò determina una profonda alterazione del diritto all'informazione come tradizionalmente inteso, così come (seppur in una certa misura) del pluralismo informativo. Inconsapevolmente, infatti, gli utenti accendono a contenuti che ritengono essere una rappresentazione quanto più esaustiva della realtà documentata. In realtà, invece, nel tempo essi sono esposti soltanto a *certe* fonti di informazione (peraltro su temi ben circoscritti) e le logiche secondo cui ciò accade sono normalmente a loro ignote[664].

La stessa sorte interessa ovviamente anche altri diritti normalmente esercitati attraverso l'utilizzo di questi strumenti, come ad esempio la libertà di associazione. Sempre più di frequente, infatti, enti e istituzioni utilizzano i *social media* per comunicare con il grande pubblico, creando in questi spazi il principale luogo di aggregazione sociale a livello nazionale e internazionale[665]. Chiaramente esistono dei canali alternativi a quelli appena descritti ma certo non si può trascurare il potenziale di questi strumenti. Rispetto a questo, dunque, ancora una volta, i sistemi di moderazione e filtraggio dei contenuti possono incidere sensibilmente sulla portata del diritto di associazione, facilitando o dissuadendo le interazioni in funzione di come sono progettati i sistemi di controllo nelle diverse piattaforme[666].

---

664 Per una panoramica sul tema, v. F. PASQUALE, *The Back Box Society,* cit., pp. 59-101.

665 Alcuni spunti sui profili costituzionali del tema (seppur analizzati nel contesto dell'ordinamento statunitense) v. J. JNAZU, *Virtual Assembly*, in *Cornell Law Review*, 2013, pp. 1093-1142, spec. pp. 1118 ss.

666 I. BROWN, *Online Freedom of Expression, Assembly, Association and the Media in Europe*, Consiglio d'Europa, *Council of Europe Conference of Ministers on Freedom of Expression and Democracy in the Digital Age*, 2013 (MCM(2013)007), pp. 15 ss.

Le preoccupazioni maggiori, tuttavia, interessano l'effettività del diritto all'eguaglianza e del principio di non discriminazione.

Negli ultimi anni, alcuni fatti di cronaca hanno messo in luce una serie di problemi già emersi in ambito commerciale, nel mercato del lavoro e – ancor più grave – nelle nel sistema giudiziario. Affidando ai sistemi di *machine learning* il compito di decidere le politiche dei prezzi al consumatore, le strategie di gestione del personale, piuttosto che la possibilità di poter accedere ad alcuni benefici nell'ambito del sistema penitenziario, si corre il rischio che le macchine, assimilando logiche e stereotipi socialmente radicati, contribuiscano a perpetrare ingiustizie e pregiudizi che, sul piano del diritto, invece si vorrebbero contrastare. Sebbene ancora manchi una vera e propria giurisprudenza su questi temi, la casistica è ormai ampia, spaziando dalla discriminazione di genere a quella etnico-raziale, fino a quella religiosa. La lista, peraltro, è destinata ad estendersi, soprattutto se si considera la casualità con cui possono essere creati i diversi *cluster* e le implicazioni che questi possono avere circa il godimento di diversi diritti sociali (come ad esempio la sanità, l'istruzione, la previdenza sociale e l'accesso al credito).

A tutto ciò si aggiunge che i diritti tradizionalmente contemplati nei testi costituzionali e delle carte internazionali sono concepiti come garanzie contro le interferenze da parte degli Stati, mentre nell'era digitale emergono nuove forme di potere, in cui convergono monopoli economici e informativi per lo più privati[667]. Ed è per tale motivo che, a livello europeo, si guarda con particolare interesse al diritto alla protezione dei dati personali e alla relativa disciplina. I principi sanciti dalla Carta di Nizza e la normativa di questo settore, infatti, astrattamente si rivolgono a *tutti* i soggetti coinvolti nel trattamento di queste informazioni, definendo implicitamente una serie di criteri per addivenire ad un equo bilanciamento degli interessi che qui si contrappongono.

---

[667] EDPS, *EDPS Opinion on coherent enforcement of fundamental rights in the age of big data,* parere del 23 settembre 2016, n. 8, p. 8.

Rispetto a questo primo approdo, tuttavia, emergono già alcune criticità. Da un lato, infatti, quanto ci si confronta con il disposto dell'art. 8 CDFEU ci si trova di fronte ad una figura dalla natura ancora molto dibattuta, spesso polarizzata sulle garanzie a tutela del rispetto della vita privata[668]. Dall'altro, i principi che ispirano la disciplina sulla protezione dei dati personali sono stati tradizionalmente intesi per una realtà in cui le operazioni di trattamento erano relativamente statiche e non particolarmente articolate, mentre ora si avverte l'urgenza di una lettura anticipatoria e dinamica delle garanzie, così da scongiurare *ex ante* l'insorgere di possibili rischi[669].

Individuate le prime categorie di diritti intercettati dalla rivoluzione dei *big data*, vi è ora da capire quali possano essere le strategie migliori per prevenire eventuali pregiudizi, concentrandosi soprattutto sull'approccio sviluppato dal reg. 679/2016 in materia di valutazioni di impatto.

### *4.2. Un approccio precauzionale al problema del rischio: le valutazioni di impatto*

In ambito giuridico i problemi legati alla gestione del rischio sono stati approfonditi da diversi punti di vista. Non è una novità che alcune attività possano essere esposte ad una alea maggiore rispetto ad altre, ed è per questo che in vari settori si sono elaborate differenti soluzioni.

In generale, si possono distinguere due tipi di situazioni: quelle che comportano una volontaria assunzione del rischio (*e.g.* il rischio contrattuale, il rischio d'impresa) e quelle in cui, invece, il soggetto si trova sottoposto al pericolo

---

668 Per un quadro si sintesi su questi temi, si veda G. GONZÁLEZ FUSTER, H. HIJMANS, *The EU rights to privacy and personal data protection: 20 years in 10 questions*, discussion paper, 14 maggio 2019 (disponibile a questo link).

669 K. DEMEZTOU, *GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved*, 2019 (contributo in corso di pubblicazione).

suo malgrado (come, ad esempio, il rischio ambientale o il rischio epidemiologico)[670].

Certo questa bipartizione non è esaustiva ma offre alcune coordinate essenziali per affrontare le questione legate al c.d. rischio tecnologico[671]. Guardando allo sviluppo delle applicazioni *data-intensive* si avverte in modo distinto come una logica *ex post* vada incontro a non pochi inconvenienti, tanto da poter rendere (seppur *in extremis*) il linguaggio dei diritti poco più che lettera morta. Il trattamento massivo di enormi quantità di dati, secondo logiche e algoritmi molto complessi, infatti, spesso si accompagna a degli elevati margini di rischio, legati non solo alla sicurezza dei sistemi ma anche al loro corretto funzionamento e all'accettabilità sociale dei loro risultati.

In tal senso, si è concordi nel ritenere che la disciplina sulla protezione dei dati personali effettivamente nasca come normativa volta a modulare i rischi legati allo

---

[670] Da un punto di vista terminologico, i concetti di «rischio» e «pericolo», così come quelli di «prevenzione» e «precauzione» non sono equivalenti. In generale, il rischio rappresenta la possibilità di trovarsi esposti ad un evento negativo di cui tuttavia è difficile quantificare l'entità e la probabilità effettiva; il pericolo, invece, indica un accadimento più che probabile, pronosticabile secondo una ben nota concatenazione causale. In virtù di ciò, si parla di prevenzione rispetto alle misure volte ad evitare un evento nefasto relativamente certo; di precauzione, invece, nelle ipotesi in cui ci si attività rispetto ad eventualità incerte sia nell'*an* sia nel *quo modo*. In queste pagine, tuttavia, per ragioni di stile, potrà accadere di trovare utilizzati i lemmi della prima coppia come se fossero sinonimi. Per un approfondimento sul tema, v. A. BARONE, *Il diritto del rischio*, Milano, Giuffrè, 2006, spec. pp. 17 ss.; R. GELLERT, *Understanding the notion of risk in the General Data Protection Regulation*, cit., p. 280.

[671] Rispetto a queste situazioni, infatti, l'atteggiamento del legislatore nel tempo ha subito importanti evoluzioni. Se in un primo momento, nello Stato liberale, per le situazioni del primo tipo vigeva un generale principio di astensione, rispetto al secondo si sono subito affermati degli specifici obblighi di prevenzione, nell'ottica di garantire attraverso la mano pubblica l'incolumità dei cittadini. In seguito, con lo sviluppo dello Stato pluralista, si è assistito ad un graduale cambiamento di questo stato di cose. Con l'istituzionalizzazione delle attività produttive e gli interventi pubblici in materia economica, diventa infatti un compito dello Stato quello di garantire adeguate condizioni per lo sviluppo della personalità del singolo, tanto da imporre l'obbligo di un regime assicurativo per lo svolgimento di alcune attività. Sempre nell'ottica di promuovere tecnologie e applicazioni allineate al principio personalista e ambientalista, in molte costituzioni ha trovato spazio la logica della precauzione, secondo cui, a fronte di attività che presentano margini di rischio particolarmente severi, possono essere imposte specifiche limitazioni onde evitare potenziali pregiudizi dovuti al c.d. *ignoto tecnologico*. Sempre in A. BARONE, *Il diritto del rischio*, cit., spec. pp. 9 ss.

sviluppo delle tecnologie dell'informazione[672]. Tuttavia, approfondendo queste prime considerazioni, non si può fare a meno di notare come il concetto possa essere declinato secondo logiche assai diverse. Se in un primo momento ci si era concentrati soprattutto su una nozione minima, riferibile soltanto alla sicurezza dei sistemi e alle misure necessarie ad assicurare l'inviolabilità dei sistemi, in seguito, questa concezione è stata gradualmente superata, includendo non solo i profili procedurali, ma anche quelli legati alle prerogative relative alla gestione dei dati, così come alla tutela della dignità e dell'identità della persona[673].

È per questo motivo che, fin da principio, il legislatore, in questi ambiti, oltre alle misure prettamente giuridiche, ha prestato attenzione anche alle soluzioni di carattere tecnico, incoraggiando l'adozione di accorgimenti utili alla tutela dei diritti già a partire dalla fase di progettazione[674]. Rifiutando le teorie che affermano la neutralità del *design*[675], in questo modo si tende a promuovere uno sviluppo più consapevole delle nuove tecnologie, così da ottenere dispositivi che, nella logica e nei risultatati, siano pienamente allineati alle aspettative sociali (anche quelle meno immediate).

Nell'ambito della protezione dei dati, pertanto, si sta cominciando ad elaborare specifiche metodologie per l'analisi e la gestione dei rischi, mettendo a punto nuove procedure che consentano di identificare efficacemente le possibili fonti, gli

---

672 R. GELLERT, *Data protection: A risk regulation? Between the risl management of everything and the precautionary alternative*, cit., pp. 4 ss. e 12 ss.; V. MAYER-SCHONBERGER, *Generational Development of Data Protection in Europe*, cit., p. 224;

673 L.A. BYGRAVE, *Data Protection Law – Approaching Its Rational, Logic, and Limits*, cit. pp. 39.

674 Alcuni interessanti riflessioni in merito in M. WARNIER, F. DECHESNE, F. BRAZIER, *Design for the Value of Privacy*, in J. VAN DEN HOVEN. P.E. VERMAAS, I. VAN DE POEL (a cura di), *Handbook of Ethics, Values, and Technological Design. Sources, Theory, Values and Application Domains*, Dorcrecht, Springer, 2015, pp. 433-446; K. YEUNG, *Desing for the Value of Regulation*, *ibidem*, pp. 447-472; R. BROWNSWORD, *So What Does the World Need Now? Reflections on Regulating Technologies*, in R. BROWNSWORD, K. YEUNG (a cura di) *Regulating technology*, Oxford, Hart Publishing, 2008; K. YEUNG, *Towards an understanding of regulation by design*, *ibidem*.

675 M. HILDELBARNDT, L. TIELEMANS, *Data protection by design and technology neutral law*, in *Computer Law & Security Review*, 29/2013, pp. 509-521, spec. pp. 511-513.

eventuali pregiudizi e le possibili soluzioni[676]. Come già ricordato, il reg. 679/2016 ha introdotto particolari obblighi per la valutazione dell'impatto dei processi che possono «presentare un rischio elevato per i diritti e le libertà delle persone fisiche»[677], incoraggiando così anche in quest'ambito una procedimentalizzare la gestione del rischio. Le novità introdotte, tuttavia, non sono affatto pacifiche. Un approccio basato sul rischio, infatti, presuppone che sia chiaro che cosa deve essere valutato e quali sono gli interessi che si intendono preservare; aspetti che, considerata l'ambigua natura del diritto alla protezione dei dati personali, possono non risultare del tutto immediati[678]. Sebbene le linee guida suggeriscano un'interpretazione ampia di quest'istituto – includendo non solo gli interessi legati alla rispetto della vita privata ma anche quelli connessi ad altre prerogative, come la libertà di espressione e di pensiero, la libertà religiosa o la libertà di movimento[679] – normalmente, quando ci si trova ad esaminare la portata dell'art. 8 CDFUE si tende a favorire una lettura orientata soprattutto ai valori della *privacy*, lasciando in secondo piano gli altri diritti tutelati dalla Carta.

Alla luce di queste considerazioni, dunque, è utile analizzare la logica che ha guidato la Corte nei suoi precedenti, onde comprendere la *ratio* che guida

---

[676] R. GELLERT, *Understanding the notion of risk in the General Data Protection Regulation*, cit., p. 280. Riprendendo gli standards elaborati dall'International Standards Organization (ISO) sulla gestione dei rischi (ISO 31000:2009 - *Risk Management Principles and Guidelines*, ora aggiornati in ISO 31000:2018 - *Risk Management Guidelines*) normalmente si distinguono due fasi: l'analisi dei rischi e la gestione dei rischi. Nella prima, si stabiliscono i criteri per l'individuazione del rischio, si descrivono quindi gli eventi che possono rientrare nella definizione e se ne valutano la probabilità e l'intensità di impatto (magnitudo). Nella seconda, invece, si identificano le possibili soluzioni, che possono concorrere a ridurre, controllare, rispondere o minimizzare il verificarsi dell'evento o le sue conseguenze. Per quanto possano essere efficaci le misure adottate, tuttavia, è molto difficile che il rischio possa essere ridotto a zero.

[677] Reg. 679/2016, art. 35, § 1.

[678] C. QUELLE, *The Data Protection Impact Assessment, or: How the General Data Protection Regulation May Still Come to Foster Ethically Responsible Data Processing*, research paper, 25 novembre, 2015 (disponibile a questo link).

[679] Gruppo Articolo 29, *Statement on the role of a risk-based approach in data protection legal frameworks* (WP218), 30 maggio 2014, p. 4 (posizioni confermate anche nelle *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679* (WP248 rev.1) del 4 ottobre 2017, p. 17).

l'interpretazione del *bill of rights* europeo. Se infatti, com'è emerso nei paragrafi precedenti, i giudici comunitari sono propensi ad estendere l'ambito di applicazione della disciplina sui dati (e così la loro competenza), diventa cruciale capire che implicazioni può avere questa "migrazione" verso l'alto del sistema di tutele sul modo in cui i diritti fondamentali sono tradizionalmente intesi, a livello europeo e nelle tradizioni costituzionali degli Stati.

### *4.3. La Corte di giustizia UE, la digital privacy…e gli altri diritti*

La Corte di giustizia non ha ancora avuto modo di sviluppare una propria giurisprudenza sui *big data* e le tecnologie *data-intensive*. Tuttavia, soprattutto negli ultimi anni, ha avuto occasione di cimentarsi spesso su temi e questioni legati alla protezione dei dati. Ciò che ha contraddistinto la dottrina dei giudici europei, in particolare, è il fatto di aver adottato in quest'ambito un approccio "forte" rispetto alla tutela dei diritti *online*, tanto da esser valso loro il titolo di garanti costituzionali dei diritti "digitali"[680].

Per approfondire la portata di queste pronunce rispetto al tema che qui interessa, sarà quindi necessario procedere per gradi, chiarendo innanzitutto che cosa la giurisprudenza identifica come "rischio" (evento) e quindi le implicazioni che questo può avere rispetto all'esercizio dei diritti fondamentali (conseguenza).

---

[680] Come ricorda H. HIJMANS, *The European Union as a constitutional guardian of internet privacy and data protection*, tesi di dottorato, 2016 (disponibile a questo link). Tuttavia, quest'approccio è valso alla Corte elogi e critiche, come emerge dalle opinioni contrastanti registrate in dottrina. O. POLLICINO, *Un* digital right to privacy *preso (troppo) sul serio dai giudici di Lussemburgo?* cit.; B. PETKOVA, *Towards an Internal Hierarchy of Values in the EU Legal Order: Balancing the Freedom of Speech and Data Privacy*, cit.; G. SARTOR, *The right to be forgotten: Balancing interests in the flux of time*, cit.; S. KULK, F. ZUIDERVEEN BORGESIUS, *Privacy, freedom of expression, and the right to be forgotten in Europe*, cit.; S.J. SCHULHOFER, *An International Right to Privacy? Be Careful What You Wish for*, in *International Journal of Constitutional Law*, 2016; B. PETKOVA, *Domesticating the 'Foreign' in Making Data Privacy Law*, in *International Journal of Constitutional Law,* 2017.

In tal senso, la percezione che i *big data* possono avere effetti dirompenti sulla vita e sui diritti delle persone è emersa soprattutto a partire dal 2012, con l'introduzione della causa *Digital Rights Ireland*. Senza dubbio, prima di allora, si era ben consapevoli del potenziale (positivo e negativo) legato all'utilizzo di queste tecnologie. Tuttavia, è solo da quel momento che questo sentore entra a far parte dell'*acquis* giurisprudenziale europeo, quando la Corte si è trovata costretta a constatare come i dati raccolti (e, in generale, oggi in circolazione)

> presi nel loro complesso, possono permettere di trarre conclusioni molto precise riguardo alla vita privata delle persone […], come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati[681]

E questo accade in una misura tale da ingenerare nelle persone una «sensazione diffusa di controllo», idonea a influenzarle in modo decisivo nell'esercizio dei loro diritti[682].

La portata di questo assunto è stata dunque elevata a parametro, tant'è che per distinguere il grado di ingerenza determinato da un certo tipo di trattamento in ragione della quantità di dati elaborati, oggi i giudici europei tendono a rifarsi proprio a questo potenziale predittivo[683].

---

[681] *Digital Rights Ireland*, sent. § 27.

[682] *Digital Rights Ireland*, conclusioni AG, § 52: «Anzitutto, non si può di certo ignorare che la sensazione diffusa di controllo che può ingenerare l'attuazione della direttiva 2006/24, è idonea a influenzare in modo decisivo l'esercizio, da parte dei cittadini europei, della loro libertà di espressione e d'informazione e che deve pertanto essere constatata anche l'esistenza di un'ingerenza nel diritto garantito dall'articolo 11 della Carta». Tuttavia, prontamente si osserva, «la Corte non dispone di elementi sufficienti per pronunciarsi a tal proposito, che tale effetto rappresenterebbe soltanto una conseguenza secondaria di un'ingerenza nel diritto al rispetto della vita privata che è oggetto, nel prosieguo, di un esame molto attento e circostanziato» (cfr. CGUE, sent. § 37). Su questo punto ci sarà comunque occasione di tornare meglio, in seguito, nel prosieguo.

[683] *Ministerio Fiscal* sent. cit., in cui, con riferimento alle misure di *data retention*, si legge che «in conformità al principio di proporzionalità […] una grave ingerenza può essere giustificata, in materia di prevenzione, ricerca, accertamento e perseguimento di un reato, solo da un obiettivo di lotta contro la criminalità che deve essere qualificata come "grave"» (sent. § 56) e, in ragion di ciò, rispetto ai dati richiesti nel giudizio *a quo*, la Corte conclude che «i dati oggetto della domanda di accesso di cui al procedimento principale consentono unicamente di collegare, nel corso di un

Se il rischio-evento può essere definito agilmente in questi termini (quanto meno nelle sue evidenze più immediate) si rivela invece più complesso stimare la portata dei rischi-conseguenza, soprattutto per quanto riguarda gli interessi che si intendono tutelare.

L'operazione in questo caso risulta più complicata soprattutto per l'incerta natura del diritto alla protezione dei dati personali, spesso associato solo ed esclusivamente ai valori della *privacy*[684].

Ciò è risultato particolarmente evidente in diverse occasioni: sia nelle decisioni in cui la Corte si è trovata a decidere sul ruolo della *data protection* nei rapporti tra Stato e cittadini, sia nei casi in cui, invece, si è pronunciata con riferimento all'attività di alcune società leader di settore. In entrambi i frangenti, infatti, i giudici europei si dimostrano affini ad una lettura focalizzata sulla tutela della vita privata, lasciando invece gli altri diritti in esame sullo sfondo, senza indugiare in troppe motivazioni.

Esaminando alcuni passaggi relativi alla funzione dell'art. 8 CDFUE nei rapporti verticali, ad esempio, nella domanda di pronuncia pregiudiziale in *Digital Rights Ireland* i giudici nazionali, oltre ai diritti sanciti dagli artt. 7 e 8 CDFUE, avevano messo in luce anche le prerogative connesse alla libertà di circolazione, alla libertà di espressione e al diritto ad una buona amministrazione[685]. La Corte,

---

determinato periodo, la o le carte SIM attivate con il telefono cellulare rubato con l'identità civile dei titolari di tali carte SIM. Senza una verifica incrociata dei dati relativi alle comunicazioni effettuate con tali schede SIM e dei dati relativi all'ubicazione, *questi dati non permettono di conoscere né la data, né l'ora, né la durata, né i destinatari delle comunicazioni effettuate* con la o le carte SIM in questione, né i luoghi in cui dette comunicazioni sono avvenute o la frequenza di esse con talune persone nel corso di un determinato periodo. *Questi dati non permettono quindi di trarre conclusioni precise sulla vita privata delle persone i cui dati sono oggetto di attenzione*» (sent. § 60, corsivo aggiunto).

[684] Su questo punto si rimanda alle riflessioni già esposte nel Capitolo 2, § 3.2.

[685] Domanda di pronuncia pregiudiziale proposta dalla High Court of Ireland l'11 giugno 2012 - *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General*, § 2, rispettivamente ai punti *i)* rispetto al diritto dei cittadini di circolare e soggiornare liberamente nel territorio degli Stati membri sancito dall'articolo 21 TFUE; *iv)* al diritto alla libertà di espressione sancito dall'articolo 11 della Carta e dall'articolo 10 della Cedu; e *v)* al diritto ad una buona amministrazione contemplato dall'articolo 41 della Carta.

tuttavia, concentrandosi soprattutto sugli interessi legate alla c.d. *digital privacy*, hanno dimostrato una certa indifferenza rispetto a tali censure, concentrandosi soltanto sulle disposizioni inerenti la tutela della sfera privata[686].

Nelle successive pronunce in materia, allo stesso modo, quando vi è stata occasione di prendere posizione sull'opportunità di minimizzare il trattamento dei dati personali conservati per finalità investigative e repressive, i giudici europei hanno confermato questo approccio «*privacy*-centrico». Considerando l'opportunità di limitare l'utilizzo dei dati ad una sorta di *small data retention*, infatti, i giudici europei di prassi suggeriscono un criterio geografico, individuato quando «autorità nazionali competenti considerino, sulla base di elementi oggettivi, [ritengano *n.d.a.*] che esiste, in una o più zone geografiche, un rischio elevato di preparazione o di commissione di atti di questo tipo»[687]. Così facendo, però, la Corte UE dimostra di privilegiare ancora una volta le esigenze di riservatezza, qui sottostimando – inconsapevolmente o meno – i rischi che l'adozione che siffatte misure possono comportare, invece, quanto al rispetto diritto non discriminazione (soprattutto etnico-religiosa)[688].

---

[686] *Digital Rights Ireland*, sent., §§ 39-40 (in cui la Corte si concentra soprattutto sui contenuti essenziali dei diritti alla protezione dei dati personali e al rispetto della vita privata) e § 71 (in cui i giudici europeo osservano come, risolte le questioni inerenti gli artt. 7 e 8 CDFUE non sia necessario soffermarsi sulle questioni relative all'art. 11 CDFUE).

[687] *Tele2 Sverige*, sent. § 111.

[688] Con questa soluzione si corre il rischio, infatti, di esporre a controllo minoranze o gruppi idealmente più esposti all'attenzione mediatica rispetto al fenomeno terroristico (cfr. G. FORMICI, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia* Ministerio Fiscal, cit., p. 470 con riferimento alle considerazioni espresse in D. FENNELLY, *Data retention: the life, death and afterlife of a directive,* in *ERA Forum*, Springer, 25 giugno 2018). Simili *escamotage*, peraltro, erano già stati cassati dalla Corte nella sua precedente giurisprudenza quando, seppur in frangenti diversi, si era esclusa la possibilità di conservare legittimamente dati personali che potessero avere un esito ingiustamente discriminatorio nei confronti di alcune categorie di persone (sent. 16 dicembre 2008, *Heinz Huber c. Bundesrepublik Deutschland* (causa C-524/06), §§ 75 e 77-81).

Circa i rischi connessi alle discriminazioni etnico-razioni e religiose legate al trattamento mirato dei dati personali si vedano inoltre, per il contesto americano, C. TORRES, A. SHAHSHAHANI, T. TAVARAS, *Indiscriminate Power: Racial Profiling and Surveillance since 9/11*, in *University of Pennsylvania Journal of Law and Social Change* 2015-16, pp. 283-310; N. CHOWDHURY*, I, Spy (But Only On You):* Raza v City of New York*, The Civil Rights Disaster of Religious and Ethnic- Based Surveillance and the National Security Excuse,* in *Columbia Human Rights Law Review,* 2014-15, pp. 278-

Pur riferendosi a parametri diversi, analoghi problemi sono emersi anche nelle cause che hanno finora coinvolto i c.d. *tech giants*[689].

Con una giurisprudenza che è stata definita da alcuni come "manipolativa", i giudici europei non solo sono stati propensi ad includere nell'ambito di applicazione della disciplina in esame qualsiasi attività abbia ad oggetto un substrato informativo[690], ma anche ad interpretare i contenuti della Carta secondo una prospettiva assiologicamente sbilanciata a favore degli artt. 7 e 8 CDFUE[691].

A far scuola, in tal senso, sono soprattutto alcuni passaggi argomentativi della sentenza *Google Spain,* che dimostrano chiaramente come la Corte UE in qualche modo contribuisce a creare una gerarchia di valori[692] rispetto a quanto previsto dal proprio *bill of rights*, lasciando nell'ombra le prerogative legate alla libertà di iniziativa

331; per il contesto europeo, M.E. GENNUSA, I. CANOR, *Il caso Kadi in tema di sicurezza*, in M. CARTABIA (a cura di), *Dieci casi sui diritti in Europa*, Bologna, Il Mulino, 2011.

[689] I riferimenti sono soprattutto alle sentenze che hanno coinvolto Google e le sue succursali europee (sent., *Google Spain SL e Google Inc.*, cit; causa *Google Inc. c. Commission nationale de l'informatique et des libertés* (CNIL), (causa C-507/17) attualmente pendente); Facebook (sent. del 6 ottobre 2015, *Maximillian Schrems c. Data Protection Commissioner* (causa C-362/14) (*Schrems I*) e causa *Data Protection Commissioner c. Facebook Ireland Limited, Maximilian Schrems* (causa C-311/18) (*Schrems II*) attualmente pendente); Youtube (sent. 14 febbraio 2019, *Sergejs Buivids* (causa C-345/17)).

[690] Da ultimo, si veda la sent. *Buivids*, in cui la Corte, pur trovandosi di fronte ad un'attività di trattamento di dati che – idealmente – poco avrebbero avuto a che fare con la dimensione privata (§ 24) ha comunque concentrato il proprio scrutinio sul solo art. 7 CDFUE, utilizzato come unico parametro per legittimare una lettura estensiva di quanto previsto dalla dir. 95/46 (§ 64 e 67).

[691] *Google Spain*, sent. § 69. Come si osserva in O. POLLICINO, *Un* digital right to privacy *preso (troppo) sul serio dai giuridici di Lussemburgo?* cit.: « A differenza di quanto fatto dall'Avvocato generale, che aveva operato un riferimento numericamente quasi equivalente tra, da una parte, gli articoli appena citati e, dall'altra parte, le disposizioni della Carta rilevanti in tema di libertà di espressione (ed accesso all'informazione) – art. 11 – e di libertà di iniziativa economica – art. 16 –, nell'apparato argomentativo della Corte entrambe le previsioni normative appena richiamate scompaiono. Nessun riferimento agli artt. 11 e 16 è rinvenibile ed il campo è lasciato interamente libero alle numerosissime citazioni presenti, invece, degli artt. 7 ed 8 della Carta» (p. 14).

[692] B. PETKOVA, *Towards an Internal Hierarchy of Values in the EU Legal Order: Balancing the Freedom of Speech and Data Privacy*, cit.

economica [693] e, soprattutto, quelle inerenti alla libertà di espressione e informazione[694].

Notissima ormai la vicenda, in questo caso i giudici lussemburghesi, dopo aver constatato come i motori di ricerca oggi godano di incredibili capacità di organizzazione e aggregazione dei contenuti – tanto da proporre un *identikit* dettagliato (ma non sempre accurato) praticamente di ogni persona[695] – osservano come in questo caso sia auspicabile trovare un equo bilanciamento di interessi. Se da un lato, infatti, vi sono le aspettative di riservatezza della persona dell'interessato, dall'altro, non si può trascurare l'interesse degli utenti di internet ad avere accesso ai contenuti disponibili *online*. Tuttavia, nel cercare «un giusto equilibrio segnatamente tra tale interesse e i diritti fondamentali della persona di cui trattasi derivanti dagli articoli 7 e 8 della Carta, la Corte conclude che «indubbiamente i diritti della persona interessata tutelati da tali articoli prevalgono, di norma, anche sul citato interesse degli utenti di Internet» [696]. Salve cioè alcune eccezioni [697], «la regola è la soccombenza del diritto (derubricato in mero interesse) all'accesso all'informazione a favore dei diritti che riguardano [invece *n.d.a.*] la protezione della sfera privata e dei dati personali degli utenti»[698].

Miglior sorte, in alcuni casi, sembra esser toccata alle aspettative al diritto alla difesa[699]. La giurisprudenza, infatti, dimostra come nel tempo l'art. 47 CDFUE stia

---

[693] *Google Spain,* conclusioni AG § 124, alla luce di quanto previsto dall'art. 16 CDFUE.

[694] *Google Spain,* conclusioni AG § 121; *Buivids*, conclusioni AG Eleanor Sharpston, 27 settembre 2018, § 19.

[695] *Google Spain*, sent. § 37.

[696] *Ibidem*, § 81.

[697] *Ibidem*, § 81, secondo cui bisognerà comunque tener conto, «in casi particolari, dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona suddetta, nonché dall'interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica».

[698] O. POLLICINO, *Un* digital right to privacy *preso (troppo) sul serio dai giuridici di Lussemburgo?* cit., p. 15.

[699] *Schrems I,* sent. § 95; sent. 4 maggio 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde contro Rīgas pašvaldības SIA "Rīgas satiksme"* (causa C-13/16), §§ 29 e 33-34; sent., 27

diventando un parametro essenziale per valutare la legittimità del trattamento dei dati personali, qualsiasi esso sia: dalla raccolta, alla cancellazione, al trasferimento verso un Paese terzo. Considerata la natura della disciplina e la portata dei diritti che questa tradizionalmente accorda all'interessato, una conclusione di questo genere sorprende fino ad un certo punto.

Tuttavia, nonostante ci sia già stato modo di osservare come, quando si affrontano le questioni relative a dati e algoritmi, ci si trovi di fronte ad una «costellazione particolarmente complessa e difficile di diritti fondamentali»[700], la Corte UE spesso afferma di non disporre di elementi sufficienti per pronunciarsi su *tutti* i diritti che possono essere intercettati dai *big data*, in quanto gli eventuali effetti negativi, a suo dire, rappresenterebbero «soltanto una conseguenza secondaria di un'ingerenza nel diritto al rispetto della vita privata»[701].

Conclusioni di questo tipo, però, sollevano non poche perplessità[702]. Nei rinvii pregiudiziali, infatti, spesso vengono in luce interessi *altri*, diversi rispetto a quelli legati alla sola tutela della sfera privata, e questo in linea con le differenti sensibilità che i giudici nazionali manifestano rispetto al rapporto tra informazioni e diritti[703].

---

settembre 2017, *Peter Puškár c. Finančné riaditeľstvo Slovenskej republiky e Kriminálny úrad finančnej správy* (causa C-73/16), §§ 36-38 e 76; in ragione di quanto sancito dall'art. 47 CDFUE.

[700] Conclusioni dell'AG Niilo Jääskinen, 25 giugno 2013, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González* (causa C-131/12), § 133.

[701] *Digital Rights Ireland*, conclusioni AG, § 52.

[702] In tal senso, alcuni primi barlumi – per quanto ancora criptici – si possono rinvenire nella recentissima sentenza del 24 settembre 2019, con cui la Corte UE è tornata a decidere sulla posizione di Google, quanto alla portata del diritto all'oblio (cfr. CGUE, sent. 24 settembre 2019, *Google LLC, venant aux droits de Google Inc. c. Commission nationale de l'informatique et des libertés (CNIL)* (causa C-507/17)) Riprendendo le riflessioni circa i rapporti tra protezione dei dati e libertà di informazione, i giudici europei, in quest'ultima pronuncia, sembrano dare maggior rilievo alla pluralità di interessi legati al trattamento delle informazioni personali. Pur non discostandosi dal suo precedente convincimento, i giudici europei non hanno infatti mancato di ribadire come sia necessario verificare attentamente, caso per caso, se e come il risultato proposto dai nuovi *media* «si riveli strettamente necessario per proteggere la libertà di informazione degli utenti di Intenet […], libertà sancita dall'articolo 11 della Carta», stabilendo comunque che, per contro, i gestori del servizio si trovino in una posizione di garanzie affinché l'immagine proposta per ciascun utente sia quanto più possibile veritiera e pertinente alla sua situazione attuale.

[703] Si veda quanto già accennato nel Capitolo 2, § 3.3., nota n. 189.

Alla luce di queste discrepanze, dunque, non è da escludere che questa giurisprudenza, a lungo andare, possa generare qualche motivo di conflitto, soprattutto quanto questa tentacolare competenza europea in materia di *data protection* finisca con il forzare gli equilibri di valore segnati dalle Costituzioni interne.

### *4.4. Il regolamento 679/2016: quali prospettive?*

Il regolamento pur non arrivando a dirimere la questione in modo chiaro, oggi sembra propendere per una visione di più ampio respiro. Il legislatore europeo, così come le autorità garanti, infatti, non manca di richiamare l'inscindibile legame che lega la protezione dei dati ad altri importanti diritti fondamentali, rifacendosi espressamente al «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»[704].

Ferme restando le perplessità accennate, dunque, in termini pratici, sono state previste una serie di garanzie volte a promuovere quest'approccio preventivo, prevedendo tanto misure di portata generale, quanto cautele più specifiche, pensate solo per i trattamenti che presentano più elevati margini di rischio.

Partendo dal considerare le prime, ad esempio, secondo quanto previsto dall'art. 25, il regolamento, ha introdotto alcuni particolare obblighi in materia di protezione *by design* e *by default.* Come ricordato, il testo non fornisce una definizione specifica delle soluzioni che prescrive introducendo questi requisiti, lasciando liberi i titolari di adottare le misure più opportune a secondo dalle specificità delle loro attività di trattamento e del contesto. Fatti alcuni accenni alle misure di

[704] Reg. 679/2016, *considerando* 4.

pseudonimizzazione e minimizzazione dei dati[705], è interessante notare come, in questi casi, in linea con i principi di trasparenza e *accountability*, il legislatore europeo tenda a rifarsi a dei modelli aperti[706]. Così come in altri campi, anche in quest'ambito esistono specifici standard tecnici cui gli operatori, di volta in volta, possono rifarsi in funzione delle loro esigenze. Tuttavia, si è preferito orientarsi non tanto verso un unico standard dato, quando ad un processo aperto e partecipativo, volto a stimolare il continuo miglioramento delle *best practices* secondo un approccio calibrato di volta in volta alle esigenze del caso specifico e ai diritti che in esso vengono in luce.

Allo stesso modo, considerando invece le misure riservate ai trattamenti esposti ad un'alea maggiore, il nuovo art. 35 ha introdotto l'obbligo di procedere a questo genere di adempimento non per qualsiasi genere di trattamento, bensì soltanto per quelli che possono presentare un «rischio elevato per i diritti e le libertà delle persone fisiche».

Come rilevato, sebbene gli ordinamenti anglosassoni già avessero sviluppato da tempo dei validi sistemi di *privacy risk assessment*, la norma in questione dunque si concentra non solo sulla riservatezza delle informazioni ma sulla protezione dei dati personali in senso ampio, idealmente aperto ad includere nella valutazione non solo le questioni inerenti il rispetto a la tutela della dimensione informativa della vita privata, bensì un più ampio ventaglio di diritti, proprio come suggerito dal Gruppo Articolo 29.

---

[705] Reg. 679/2016, art. 25, § 1: «[…] 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»

[706] A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva*, in G. FINOCCHIARO (diretto da), *Il nuovo regolamento europeo sulla privacy*, cit., p. 307.

Considerata la complessità dell'ambiente in cui si calano queste previsioni, non mancano dunque alcune perplessità, soprattutto per quanto riguarda lo sviluppo e l'utilizzo delle applicazioni *data-intensive*.

In particolare, emergono alcuni interrogativi relativi alla copertura delle garanzie *by design* e *by default*, legate soprattutto alla natura degli interessi che si pretende di tutelare. Come accennato, infatti, non è ancora pacifico quale sia il perimetro del diritto alla protezione dei dati personali, così come l'equilibrio che regola i rapporti tra detta figura e gli altri diritti fondamentali comuni alla tradizione costituzionali dell'Unione e degli Stati membri. In particolare, vi è da capire se i profili di rischio che queste misure sono atte a scongiurare riguardino prevalentemente le questioni legate alla sicurezza, la segretezza e la minimizzazione dei dati – orientandosi così soprattutto verso i valori della *privacy* – oppure se ambiscano ad avere un più ampio respiro, aperto a tutti i principi fondamentali della *data protection* – come ad esempio la correttezza e la trasparenza – anch'essi da incorporare quindi nelle tecnologie adottate e implementanti poi per impostazione predefinita.

A ciò si aggiunge, peraltro, un ulteriore elemento di perplessità. Il regolamento suggerisce il coinvolgimento dei produttori e dei fornitori senza però introdurre alcun vincolo in tal senso[707]; una mancanza critica sotto diversi punti di vista, soprattutto se si considerano le posizioni che questi soggetti rivestono nello sviluppo tecnico dei dispositivi e dei servizi che propongono e di cui molte parti

[707] Reg. 679/2016, *considerando* 78: « In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati» (quarto periodo).

comunemente si avvalgono per i più diversi scopi[708]. L'art. 25, limitandosi a prevedere obblighi in capo al titolare soltanto presuppone dunque che chiunque si avvalga di utilità di uso assai comune nell'ambito della propria attività – come ad esempio il *cloud* o *social network* – si assuma la responsabilità delle proprie scelte. In questo, però, egli non può effettivamente concorre alla definizione delle impostazioni tecniche e delle *policy* relative alla protezione dei dati, creando così una forte frattura tra forma e realtà circa i rapporti tra i diversi soggetti che concorrono all'utilizzo delle informazioni trattate attraverso questi canali[709].

Ugualmente, guardando alle previsioni relative al *data protection impact assessment,* nonostante i suggerimenti per una lettura estensiva della norma, il fatto di aver imposto la valutazione di impatto soltanto per alcuni casi specifici (e non per tutti) potrebbe risultare una scelta non del tutto condivisibile. Pensando soprattutto all'impiego dei *big data,* in primo luogo, infatti, non tutti i trattamenti in questione necessariamente ricadono nelle categoria sopraindicate, ammettendo quindi la possibilità che, in alcuni casi, delle operazioni comunque sensibili non siano accompagnate *ex lege* dalle debite cautele. A ciò si aggiunge che la valutazione di impatto sulla protezione dei dati, per come risulta formulata la prescrizione, non presuppone valutazioni etiche ulteriori. Questa sembra concentrarsi solo sugli obiettivi di *data protection*, senza dare indicazioni univoche in merito ai criteri di bilanciamento con i diritti e gli interessi che qui si contrappongono, né circa l'analisi dell'impatto etico-sociale derivanti dall'uso dei dati, lasciando così in secondo piano la dimensione collettiva[710].

---

[708] S. CALZOLAIO, L. FEROLA, V. FIORILLO, E.A. ROSSI, M. TIMIANI, *La responsabilità e la sicurezza del trattamento*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., p. 175.

[709] Per un ampio approfondimento su questi temi si rimanda a B. VAN ALSENOY*, Data Protection Law in the EU*, cit.

[710] A. MANTELERO, *La* privacy *all'epoca dei* Big Data*,* in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di)*, I dati personali nel diritto europeo*, cit., pp. 1201 ss.

Tutto ciò considerato, dunque, è d'obbligo sottolineare come, se osservate termini generali ed astratti, le novità introdotte costituiscono senz'altro un punto di svolta nell'evoluzione della disciplina sulla protezione dei dati personali. Il fatto di aver privilegiato un approccio di preventivo, l'istituzionalizzazione delle misure di protezione *by design* e *by default* e la previsione di specifiche valutazione di impatto per le operazioni ad alto rischio, certo documentano un graduale cambio di mentalità in questa materia. E tuttavia, per come specificamente formulate, le norme in questione evidentemente rappresentano soltanto un punto di partenza; le linee di tensione di un disegno che, con il tempo, dovrà essere ampliato e portato a compimento, avendo a mente soprattutto le specificità dei singoli settori e delle diverse tecnologie.

## 5. Trasparenza: per un uso "costituzionalmente orientato" dei *big data*

Oltre a prevedere forme di tutela *by design* e *by default* e a prescrivere, ove dovute, specifiche valutazioni di impatto, per affrontare i problemi appena accennati, il reg. 679/2016 ha infine il merito di specificare meglio la cornice normativa destinata a disciplinare nello specifico l'utilizzo dei *big data analytics*, introducendo nuove definizioni e predisponendo una normativa *ad hoc* per inquadrare adeguatamente questi fenomeni tecnologici.

In tal senso, uno dei punti di maggior interesse riguarda proprio i margini di discrezionalità concessi al legislatore nazionale. Su fronti così sensibili, infatti, la possibilità di completare quanto previsto a livello europeo è guardata con particolare attenzione, in quanto l'esperienza di alcuni può fornire utili spunti di sviluppo per il legislatore comunitario, così come quelli nazionali.

L'intento di queste ultime pagine, dunque, è quello di analizzare nel dettaglio quanto previsto dal regolamento per promuovere un utilizzo dei *big data* allineato

con i diritto fondamentali. Ci si concentrerà dapprima sulle le nozioni di «profilazione» e «decisione automatizzata», anche attingendo dalle linee guida all'uopo predisposte dal Gruppo Articolo 29. Ci si soffermerà quindi sul quadro generale delle garanzie previste a livello europeo, analizzando con attenzione quanto sancito dall'art. 22 del GDPR, unitamente a quanto disposto dai *considerando* 63 e 71. Infine, si analizzeranno brevemente alcune esperienze nazionali, evidenziando come vari ordinamenti stiano facendo fronte ai problemi legati alla "costituzionalità" degli algoritmi.

L'obiettivo è quello di approfondire le considerazione relative alle figure rimediali approntate dal regolamento in questi ambiti, esaminando dove la pregressa giurisprudenza sui diritti fondamentali possa contribuire ad integrare il nuovo sistema di tutele fino al riconoscimento di un diritto alla "spiegabilità" (*explainability*) degli algoritmi.

### *5.1. Big data, profilazione e decisioni automatizzate: nuove definizioni*

Guardando alle realtà che si aprono con l'avvento dei *predictive analytics* e del *machine learning*, il primo passo fatto dal legislatore europeo in occasione della riforma è stato quello di specificare meglio la portata di alcuni concetti.

In particolare, vengono in evidenza quelli che riguardano le nozioni di «profilazione», di «processo decisionale basato su profilazione» e «decisione basata *unicamente* sul trattamento automatizzato»; tutte fattispecie che nella precedente normativa avevano avuto uno spazio ben più circoscritto.

Per questo motivo, è opportuno indugiare qualche istante su queste novità poiché consentono di ragionare a fondo sui trattamenti maggiormente esposti al rischio indicando i rimedi e le garanzie più opportune[711].

In tal senso, la prima definizione che si incontra scorrendo il testo del reg. 679/2016 è quella riportata all'art. 4, n. 4, relativa al concetto di profilazione. Può essere infatti ricondotta a tale categoria

> qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica

È quasi superfluo notare come la descrizione appena accennata sia in grado di intercettare diversi aspetti dei sistemi oggetto di questi ultimi paragrafi. La definizione, infatti, tende ad individuare proprio quella categoria di operazioni attraverso le quali non ci si limita alla sola classificazione degli individui secondo una serie di parametri prestabiliti. Essa invece guarda ad un processo valutativo[712] che, basandosi sull'elaborazione di un modello attraverso l'analisi automatizzata dei dati,

---

[711] Gruppo Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679* (WP251 rev. 1), versione aggiornata al 6 febbraio 2018. Nelle linee guida, infatti, si specifica come «errori o distorsioni nei dati raccolto o condivisi oppure un errore o una distorsione nel processo decisionale automatizzato possano comportare: classificazioni errate e valutazioni basare su proiezioni imprecise che incidono negativamente sulle persone fisiche» (p. 31), ragion per cui, il reg. 679/2016 ha introdotto una serie di previsioni volte a garantire che la profilazione e il processo decisionale automatizzato «non siano utilizzati in maniera tale da avere un impatto ingiustificato sui diritti delle persone» prevedendo, ad esempio: requisiti specifici di trasparenza e correttezza; maggiori obblighi in termini di responsabilizzazione; basi giuridiche specifiche per il trattamento; il diritto delle persone fisiche di opportisi alla profilazione (e segnatamente alla profilazione per finalità di marketing) e la necessità di effettuare una valutazione di impatto sulla protezione dei dati personali (p. 6).

[712] Secondo le Linee guida appena citate nella nota precedente, l'elemento dirimente per poter qualificare un trattamento «profilazione» e non mera «classificazione» è appunto la finalità valutativa, proprio come suggerito dal tenore letterale della norma. «L'uso del verbo "valutare" – infatti – suggerisce che la profilazione implichi una qualche forma di valutazione o giudizio in merito ad una persona; «la semplice classificazione di persona basata su caratteristiche note quali età, sesso, e altezza *non determina necessariamente profilazione*» (p. 7).

porti all'applicazione dei profili ottenuti ad una persona fisica per individuarne tratti del comportamento presenti o futuri[713].

Il secondo concetto chiave proposto dalla normativa, riguarda invece le decisioni automatizzate. Come si legge all'art. 22, § 1, del regolamento, in questo caso si ha a che fare con una decisione

> basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che [riguardino o incidano *n.d.a.*] in modo analogo significativamente sulla sua persona

La norma non indugia in ulteriori precisazioni ma comparando attentamente il tenore letterale delle due definizioni è necessario prestare particolare attenzione a tre passaggi, concentrandosi sul fatto che la profilazione, in generale, copre «*qualsiasi forma* di trattamento automatizzato» mentre i sistemi di *automatic decision-making* si riferiscono a processi basati «*unicamente* sul trattamento automatizzato, compresa la profilazione» (quando nel caso).

Procedendo con ordine, si possono fare le seguenti osservazioni. L'art. 4, n. 4, reg. 679/2016, riferendosi a «*qualsiasi* forma di trattamento automatizzato», tende ad ampliare il novero delle fattispecie considerate. Sono infatti da ritenersi incluse nel perimetro della norma tutte le operazioni che, *in toto* o in parte, presentano questa caratteristica di automazione, *senza pretesa di esclusività*, ammettendo quindi anche i

---

[713] Quanto alle fasi di profilazione, ci si è rifatti alla descrizione proposta dal Consiglio d'Europa, nella raccomandazione CM/Rec(2010)13 del Comitato dei Ministri agli Stati Membri sulla protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione, adottata dal Comitato dei Ministri il 23 novembre 2010 in occasione del 1099mo incontro dei Rappresentanti dei Ministri. Nell'all. 1, si legge: «profiling, as understood in the context of this recommendation, takes place in three technically distinct stages: a stage during which digitised observations regarding individuals' behaviour or characteristics are collected and stored on a large scale (data warehousing). The resulting data may be nominative, coded or anonymous; a stage during which these data are analysed and "probed" (data mining) permitting the determination of correlations between different behaviours/characteristics and other behaviours or characteristics; an inference stage during which, on the basis of certain observable behavioural variables or characteristics specific to a generally identified individual, new past, present or future characteristics or behavioural variables are deduced.» (§ 38, p. 25).

processi che prevedono forme di profilazione automatizzata come passaggio intermedio in un *iter* cui partecipano anche decisori umani.

L'art. 22, § 1, invece si rifà al caso opposto, circoscrivendo l'ambito di applicazione della disposizione alle decisioni basate ««*unicamente* sul trattamento automatizzato». Questa seconda previsione si rifà quindi alle situazioni nelle quali il risultato proposto dalla macchina rappresenti la risposta ultima: ai casi in cui casi, cioè, *sia l'algoritmo a "decidere"*, senza alcuna previa e significativa valutazione umana[714].

Considerata questa prima distinzione, che in qualche modo rappresenta i due casi estremi, la normativa permette infine di individuare anche altre due categorie che potremmo definire residuali. Da un lato, vi sono le ipotesi in cui la profilazione automatizzata costituisca una componente di un procedimento decisionale più complesso cui partecipano anche altri soggetti, unendo così la componente valutativa tecnologica a quella umana. Dall'altro, invece, vi sono le ipotesi in cui le operazioni di *profiling* costituiscono un procedimento autonomo e basato unicamente sul trattamento automatizzato di dati personali, proprio come richiesto dall'art. 22, § 1 e comportando così un'ulteriore qualificazione delle attività in esame, innalzando i relativi livelli di tutela.

In sintesi, dunque, profilazione e *automated decision-making* possono configurarsi sia come attività distinte sia come attività coordinate; nell'un caso la finalità del trattamento sarà la *valutazione* mentre nell'altro la *decisione* vera e propria.

Tutto ciò, però, non è dirimente sul piano delle tutele: a segnare un significativo scarto è infatti l'ultimo fattore, considerato che, sempre più di frequente, ci si trova di fronte ad operazioni *completamente* automatizzate. Così,

---

[714] Gruppo Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit. p. 9. Per un approfondimento sul senso delle definizioni si veda anche O. SESSO SARTI, *Profilazione e trattamento dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologia e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, cit., pp. 585 ss.

mentre per le operazioni di calcolo inserite in un procedimento decisionale ordinario – cioè a supporto di un decisore umano – si applicheranno le normali garanzie previste dal regolamento, è solo per le operazioni basate unicamente sul trattamento automatizzato che la normativa prevede un particolare regime di protezione, dettato dalla maggiori rischi tecnici che possono interessare tali sistemi.

### *5.2. Il quadro generale delle garanzie previste dal reg. 679/2016*

Alla luce delle considerazioni esposte, si può passare ad analizzare il quadro delle garanzie, andando a distinguere il diverso regime di protezione previsto dal reg. 679/2016 per i sistemi di profilazione e per i processi di *automatic decision-making*.

Come puntualmente spiegato dalla linee guida del Gruppo Articolo 29, si possono individuare essenzialmente due diversi livelli di tutela: da un lato, le garanzie ordinarie a favore di tutti i trattamenti che implichino una qualche forma di trattamento automatizzato; dall'altro, invece, quanto previsto appositamente dagli artt. 15 e 22 per i sistemi decisionali completamenti autonomi[715].

Chiaramente in ogni caso andranno rispettate le regole che discendono dai principi fondamentali della *data protection*. Attingendo cioè da quanto previsto soprattutto dagli artt. 5 e 6, reg. 679/2016, il *profiling* quanto le decisioni algoritmiche devono essere utilizzati nel rispetto dei dettami di trasparenza, liceità e correttezza[716]. Dal momento che gli interessati, infatti, spesso non sono a conoscenza di questo tipo di attività (o comunque faticano a realizzare le

[715] Da un punto di vista terminologico, tuttavia, questa formulazione richiede qualche precisazione. Quando si parla di sistemi decisionali completamente autonomi, infatti, si possono distinguere almeno due categorie: da un lato, quelli che sono in grado di concludere il procedimento in modo autonomo sulla base di una serie di criteri predefiniti; dall'altro, invece, quelli che sono in grado di selezionare autonomamente anche i parametri decisionali, anche modificandoli nel corso del tempo per ottimizzare le proprie prestazioni tecniche.

[716] Cfr. reg. 679/2016, art. 5, § 1, lett. a) e Gruppo Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit. p. 10.

implicazioni che possono derivarne) è necessario che questi siano messi nella condizione di aver contezza di quanto accade, imponendo così al titolare di fornire loro informazioni concise, trasparenti, intelligibili e facilmente accessibili[717], così che questi (eventualmente) possano attivarsi per verificare la puntualità dei risultati che li riguardano[718].

A ciò si aggiungono poi, le questioni relative alle finalità[719] del trattamento e alla possibilità che le stesse informazioni possano essere conservate e utilizzate anche per scopi ulteriori e diversi da quelli inizialmente dichiarati[720]. In tal senso, riprendendo una serie di fattori già identificati in precedenza[721], il titolare è tenuto a vagliare accuratamente la compatibilità tra i fini originari e quelli sopravvenuti, prestando particolare attenzione alle informazioni fornite all'interessato a suo tempo. Dovranno pertanto essere tenuti in debita considerazione il rapporto tra le diverse finalità considerate, il contesto in cui i dati sono stati raccolti, le ragionevoli aspettative dell'interessato rispetto al loro utilizzo, la natura dei dati in questione e l'impatto degli ulteriori trattamenti sul *data subject,* provvedendo ad apportare in ogni

---

[717] *Ibidem*. Uno degli aspetti rispetto al quale come si vedrà sono improntati soprattutto i sistemi nazionali. I limiti del consenso e della

[718] Come si osserva nelle Linee guida appena citate «la profilazione può essere iniqua e creare discriminazioni, ad esempio negando l'accesso a opportunità di lavoro, credito o assicurazione oppure offrendo prodotti finanziari eccessivamente rischiosi o costosi» (p. 11), in questo pregiudicando l'interessato non solo rispetto al godimento dei suoi diritti ma anche rispetto ad interessi di natura più generali come, per l'appunto, la definizione dei prezzi o le condizioni di accesso a servizi e posizioni.

[719] Reg. 679/2016, art. 5, § 1, lett. b.

[720] Sui limiti di quest'impostazione, si vedano, in generale, A. MANTELERO, *La privacy all'epoca dei big data*, in V. CUFFARO, R. D'ORAZIONE, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit.; e, più nello specifico, N. FORGÓ, S. HÄNOLD, B. SCHÜTZE, *The Principle of Purpose Limitation and Big Data*, in M. CORRALES, M. FENWICK, N. FORGÓ (a cura di), *New Technology, Big Data and the Law*, Singapore, Springer, 2017, pp. 17-42.

[721] Il Gruppo Articolo 29 aveva già avuto occasione di soffermarsi con delle specifiche indicazioni, definendo peraltro una testa di ponte per coordinare quanto previsto dalla precedenti dir. 95/46 e dal nuovo regolamento, all'epoca in fase di discussione (cfr. *Opinion 03/2013 on purpose limitation*, WP 203, 2 aprile 2013; testo disponibile soltanto il lingua inglese). Analizzando, in particolare, i problemi legati all'utilizzo dei *big data* e degli *open data*, aveva individuato una serie di condizioni per valutare la compatibilità dei nuovi fini con quelli inizialmente dichiarati al momento della richiesta di consenso (pp. 35 ss. e all. 2).

caso le garanzie necessarie ad evitare ogni indebita conseguenza in capo a quest'ultimo[722].

Non possono mancare, quindi, alcune considerazioni circa i principi di minimizzazione [723] ed esattezza [724] dei dati trattati, nonché sui limiti di conservazione[725]; una serie di assunti messi fortemente alla prova da flussi di dati – per così dire – alluvionali.

Pur trattandosi di *dataset* enormi e (potenzialmente) in continua evoluzione[726], il legislatore, per il tenore letterale delle norme, sembra comunque pretendere l'applicazione di questi principi anche ai sistemi di *big data*. In primo luogo, si prevede che il titolare sia in grado di «spiegare in maniera chiara e giustificare la necessità della raccolta e della conservazione dei dati personali», suggerendo comunque, in alternativa, l'opportunità di «prendere in considerazione l'utilizzo di dati aggregati, anonimizzati o (laddove ciò consenta una protezione sufficiente) pseudonimizzati per la profilazione»[727]. Inoltre, chi di dovere ha il compito di verificare l'esattezza delle operazioni «in tutte le fasi del processo di profilazione, in particolare quando: raccoglie i dati; analizza i dati; crea un profilo per una persona o applica un profilo per prendere una decisione su una persona»[728].

Infine, dal momento che gli algoritmi di *machine learning* richiedono fasi di *training* su grandi volumi di informazioni, vengono poste particolari condizioni circa i periodi di conservazione dei dati. Nonostante, infatti, vi possano essere considerevoli vantaggi dalla creazione di grandi *dataset*, «il titolare del trattamento deve rispettare il principio di minimizzazione dei dati all'atto della raccolta e

---

[722] Gruppo Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit. p. 12.

[723] Reg. 679/2016, art. 5, § 1, lett. c).

[724] *Ibidem*, lett. d).

[725] *Ibidem*, lett. e).

[726] Considerazioni già esposte: dati dai dati.

[727] Gruppo Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit. p. 13.

[728] *Ibidem*.

assicurare che i dati non siano conservati per un periodo superiore a quello necessario e proporzionato alle finalità per le quali i dati vengono trattati»[729]. Inoltre «la politica di conservazione del titolare del trattamento dovrebbe tenere conto dei diritti e delle libertà delle persone fisiche», assicurandosi «che i dati rimangano aggiornati durante il periodo di conservazione in maniera da ridurre il rischio di inesattezze»[730].

Lo stesso ragionamento vale per le basi giuridiche del trattamento. Come in ogni altro caso, il *profiling*, e così gli altri sistemi che presentino una qualche forma di valutazione, sono ammessi con il consenso dell'interessato, quanto necessari all'esecuzione di un contratto o se indispensabile per adempiere ad un obbligo legare, per la salvaguardia di interessi vitali o per l'esecuzione di un compito di interesse pubblico o comunque connesso all'esercizio di pubblici poteri[731]. Ultimo ma non ultimo, la profilazione sarà ammessa quando necessaria per il perseguimento di un interesse legittimo del titolare o di terzi, fermo restando che al *data controller* spetterà il compito di procedere ad un'attenta valutazione per verificare se i diritti e le libertà fondamentali dell'interessato non prevalgano sui propri interessi, considerando, caso per caso, l'incidenza del livello di dettaglio e della completezza del profilo, gli effetti del trattamento sul destinatario e le garanzie all'uopo approntate[732].

---

[729] *Ibidem.*

[730] *Ibidem*.

[731] Reg. 670/2016, art. 6, § 1 e Gruppo Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit. pp. 14-15.

[732] Ultima op. cit. p. 16. A queste si aggiungo peraltro le ulteriori considerazioni proposte dal regolamento medesimo quanto agli interessi legittimi del titolare del trattamento o dei terzi, che – come previsto dal *considerando* 47 – possono comprendere, ad esempio, stesso Gruppo Articolo 29. A riguardo, ragionando sulla vera essenza del diritto all'autodeterminazione informativa, non mancano alcuni *caveat* quanto all'effettività delle volontà espresse dall'interessato. Le Linee guida, infatti, mettono in evidenza come il più delle volte «la profilazione [possa] non essere trasparente [poiché] spesso si basa su dati derivati o desunti da altri dati, anziché su dati forniti direttamente dall'interessato»[732]. In ragion di ciò, dunque, si ritiene che «il consenso non [sia] sempre una base appropriata per il trattamento»[732] e, in ogni caso «gli interessati dovrebbero disporre di sufficienti

Sul fronte rimediale, invece, all'interessato spetteranno tutti i diritti generalmente riconosciuti dal nuovo *bill of rights* introdotto dal regolamento.

In tal senso, nel caso in cui sia presente una qualche forma di trattamento automatizzato, il titolare ha innanzitutto l'obbligo di «spiegare in maniera chiara e semplice alle persone interessate come funziona la profilazione o il processo decisionale automatizzato» [733], garantendo così un generale principio di conoscibilità[734] per tutte le attività qui in esame.

A questo si aggiungono le garanzie legate al diritto di accesso[735], che consente all'interessato di ottenere informazioni dettagliate non solo sulle categorie di dati utilizzate per creare il profilo, ma anche di accedere «alle informazioni sul profilo stesso e ai dettagli dei segmenti nei quali l'interessato è stato inserito»[736] (un passaggio particolarmente significativo, soprattutto per quanto riguarda la creazione automatizzata dei *clusters*[737]).

Sollevano poi particolare interesse i diritti che permettono al *data subject* di intervenire nelle attività del titolare, finanche – in qualche modo – a prendervi parte.

---

informazioni pertinenti sull'uso previsto e sulle conseguenze del trattamento in maniera da assicurare che il consenso fornito sia frutto di una scelta informata»[732].

[733] Reg. 679/2016, artt. 13 e 14 e Gruppo Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit. p. 18.

[734] Cfr. A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 1/2019, p. 98.

[735] Reg. 679/2016, art. 15.

[736] Gruppo Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit. p. 19.

[737] Nei processi decisionali automatizzati, infatti, la profilazione può avvenire non tanto sulla definizione di un profilo preimpostato, quanto sull'individuazione casuale di determinate caratteristiche che i dati "dimostrano" correlate tra loro. A differenza del passato, dunque, le operazioni di *clustering* potrebbero avvenire sulla base di criteri ignoti agli programmatori stessi, perché adottati dal sistema nel corso delle operazioni necessarie a migliorare il proprio rendimento nei perseguimento dei suoi obiettivi. A. MANTELERO, *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection*, in *Computer Law & Security Review*, 32/2016, pp. 238-255 (spec. pp. 241 e 145) e A. MANTELERO, *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era*, in B. VAN DER SLOOT, L. FLORIDI, L. TAYLOR (a cura di), *Group Privacy*, Verlag, Springer, 2017, pp. 139-158 (spec. pp. 145-146)

Si tratta essenzialmente delle ipotesi in cui il regolamento ammette il ricorso alla rettifica e alla cancellazione dei dati o alla limitazione del loro trattamento. Considerata infatti la natura previsionale delle attività in oggetto, queste prerogative (quanto meno teoricamente) innanzitutto, consentono all'interessato di verificare l'esattezza e la pertinenza dei dati di *input* e di *output*, nonché la correttezza delle operazioni e il funzionamento dell'algoritmo (e le sue eventuali lacune). Questi, inoltre, ha il diritto di chiedere la limitazione del trattamento in ogni fase del processo di profilazione, così come di opporvisi a motivo della sua situazione particolare.

Tuttavia, vanno rilevate alcune restrizioni. Il diritto di accesso, il diritto di rettifica, così come il diritto di opposizione, infatti, incontrano i limiti dettati dalle prerogative legate, da un lato, alla tutela della proprietà intellettuale e dei segreti industriali[738] e, dall'altro, ai legittimi interessi del titolare che possono prevalere sui diritti e libertà fondamentali dell'interessato[739].

---

[738] L'esercizio di tali diritti, infatti, ricorda il reg. 679/2016 e il Gruppo Articolo 29, «non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software», fermo restando che «tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni. Se il titolare del trattamento tratta una notevole quantità d'informazioni riguardanti l'interessato, il titolare in questione dovrebbe poter richiedere che l'interessato precisi, prima che siano fornite le informazioni, l'informazione o le attività di trattamento cui la richiesta si riferisce» (cfr. *considerando* 63; Gruppo Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit. p. 19).

[739] Allo stesso modo, il Gruppo Articolo 29 evidenzia come il bilanciamento tra gli interessi che in questi casi possono contrapporsi spetti comunque al titolare del trattamento, il quale, caso per caso, dovrà verificare (*a*) l'importanza della profilazione per i propri fini particolari e (*b*) l'impatto di tale attività sugli interessi, i diritti e le libertà dell'interessato. Un primo passo avanti, rispetto a quanto previsto dalla dir. 95/46 riguarda il fatto che oggi l'onere della prova di dimostrare l'esistenza di motivi legittimi e cogenti spessa al *controller* e non più al *data subject* (cfr. Gruppo Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit. p. 20-21).

### *5.3. Sull'esistenza di un nuovo (e controverso) diritto ad una spiegazione*

Delineato il quadro delle garanzie previste a titolo generale per il *profiling* e per le decisioni che, in qualche modo, si basano sulle operazioni di profilazione, si considerare le disposizioni previste specificamente per le decisioni basate *unicamente* sul trattamento automatizzato.

Nonostante l'art. 15 della direttiva "madre", a riguardo, avesse già introdotto alcune limitazioni[740], quanto disposto dall'art. 22 del reg. 679/2016 affronta le questioni legate alle attività di *automatic decision-making* con una contezza ben diversa, soprattutto nel tentativo di tenere il passo con i recenti sviluppi del *machine learning*.

Procedendo per gradi, la nuova norma, in termini analoghi alla precedente, esordisce affermando innanzitutto un «diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente» sulla persona dell'interessato[741].

---

[740] Da un punto di vista squisitamente letterale, basta confrontare le due norme per cogliere l'evidente evoluzione della disciplina. L'art. 15, dir. 95/46, infatti, si limitava a prevedere che «qualsiasi persona [ha] il diritto di non essere sottoposta ad una decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità, quali il rendimento professionale, il credito, l'affidabilità, il comportamento, ecc.» ammettendo come uniche eccezioni le ipotesi in cui la decisione (*a*) fosse presa nel contesto della conclusione o dell'esecuzione di un contratto o (*b*) fosse autorizzata da una legge che precisi i provvedimenti atti a salvaguardare un interesse legittimo della persona interessata», aggiungendo poi, nei *considerando*, che «una persona deve godere del diritto d'accesso ai dati che la riguardano e che sono oggetto di trattamento, per poter verificare, in particolare, la loro esattezza e la liceità del trattamento; che, per le stesse ragioni, le persone devono avere inoltre il diritto di conoscere la logica su cui si basa il trattamento automatizzato dei dati che le riguardano, perlomeno nel caso delle decisioni automatizzate di cui all'articolo 15, paragrafo 1; che tale diritto deve lasciare impregiudicati il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software; che ciò non dovrebbe comunque tradursi nel rifiuto di fornire qualsiasi informazione alla persona interessata» (*considerando* 41). Il reg. 679/2016, invece, come ci sarà modo di approfondire nelle prossime pagine, ha ampliato la portata di queste garanzie e dei relativi criteri interpretativi.

[741] Reg. 670/2016, art. 22, § 1.

Analizzando il contenuto di questa prima disposizione, la dottrina, in un primo momento, si è interrogata sulla natura della situazione giuridica soggettiva descritta, divisa tra il dubbio se ci trovasse di fronte ad un vero e proprio diritto (rispetto al quale l'interessato avrebbe avuto l'onere di attivarsi sua sponte) oppure di un divieto di carattere generale.

In tal senso, il Gruppo Articolo 29 ha chiarito che, sebbene il legislatore lo configuri come un diritto, quanto disposto dall'art. 22, sancisce in realtà un generale *divieto* nei confronti dei sistemi di decisione basati unicamente su trattamenti automatizzati[742]; e questo perché interpretando la norma «come un divieto piuttosto che come un diritto da invocare significa che le persone sono automaticamente protette dagli effetti potenziali che questo tipo di trattamento può avere»[743] a prescindere dalla contezza che di esse il soggetto possa avere.

Chiarito questo punto, è stato necessario approfondire gli elementi della fattispecie tratteggiata dalla disposizione in esame, nonché le ipotesi in cui questa individua delle eccezioni al divieto. Quanto al primo dei due aspetti, si tratta di capire quando una decisione possa definirsi «basata *unicamente* sul trattamento automatizzato»; elemento distintivo della fattispecie in questione che sostanzialmente giustifica un *quid pluris* sul piano delle tutele.

Queste forme di *decision-making* – come già ricordato – si riscontrano ogni qual volta non vi sia alcun coinvolgimento umano nel processo decisionale. Sono quindi inclusi tutti i casi in cui l'operatore non abbia alcuna influenza effettiva, evitando così che possa essere eluso il contenuto del divieto con interventi soltanto simbolici[744].

---

[742] Gruppo Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit. p. 21.

[743] *Ibidem*, p. 22.

[744] *Ibidem*, p. 23. Le Linee guida proseguo inoltre specificando che per individuare l'effettivo contributo degli operatori umani al processo decisionale automatizzato e le fasi in cui questo può aver luogo, il titolare del trattamento dovrà procedere – se del caso – alle necessarie valutazioni di impatto, così come previsto dall'art. 35, reg. 679/2016.

Per quel che invece riguarda gli effetti del trattamento in questione, la norma richiedere che questi siano in grado di «produrre effetti giuridici» in capo al *data subject*, o comunque di incidere in modo significativo nella sfera di interesse di quest'ultimo.

Evidentemente, una simile formulazione ha come primo scopo quello di includere nel perimetro della disciplina soltanto quei trattamenti idonei a produrre un impatto particolarmente grave. Tuttavia, le due ipotesi indicate dalla norma meritano particolare attenzione. L'obiettivo del regolamento, infatti, non è soltanto quello di aver cura delle eventuali limitazioni dei diritti veri e propri ma di considerare anche i risultati che possono influire sullo status dell'interessato, limitandone la libertà di scelta e le eventuali *chance*. I casi possono essere i più diversi: dai pregiudizi che possono limitare la libertà di associarsi ad altre persone, di votare nelle consultazioni nazionali o di intraprendere le vie legali, alla cancellazione di un contratto, la negazioni di una qualche prestazione sociale, piuttosto che il rifiuto di essere ammesso in un Paese o la negazione della cittadinanza[745].

Analizzati gli elementi costitutivi del divieto, l'art. 22 prosegue individuando tre diverse eccezioni. È così consentito l'utilizzo di processi decisionali completamente automatizzati nei casi in cui questi siano necessari per la conclusione o l'esecuzione di un contratto, quando autorizzati dal diritto europeo o dalla legge di

---

[745] Questi i principali esempi riportati dalle Linee guida qui in esame. Non vanno peraltro sottovalutate le conseguenze negative che possono derivare in capo all'interessato quanto all'esercizio della libertà di espressione e di informazione. I filtri con cui lavorano i motori di ricerca, piuttosto che i sistemi di moderazione automatica dei contenuti promossi dalla piattaforme *social* rappresentano infatti altre nuove insidie; e questo a riprova dei maggiori effetti che legano la protezione dei dati personali agli altri diritti fondamentali tutelati dalla Carta di Nizza e dalle Costituzioni nazionali. Si è comunque ben consapevoli del fatto che rimane comunque difficile stabilire in modo univoco quando un trattamento sia effettivamente in grado di incidere in modo sufficientemente significativo sulla sfera giuridica dell'interessato; ragione che ha indotto il Gruppo Articolo 29 a specificare ulteriormente la casistica, invitando ad avere la massima attenzione soprattutto per le alterazioni che possono determinare nocumento per le minoranze e le categorie di personale più vulnerabili. Cfr. T. SHAMDY, *The New Social Contact: Facebook's Community and Our Rights*, in *Boston International Law Review*, 2019 (*forthcoming*), *passim*; K. KLONIC, *The New Governors: The people, rules, and process governing online speech*, in *Harvard Law Review*, 2018.

uno Stato membro o quando comunque vi sia stato il consenso esplicito dell'interessato[746].

Ammettendo delle ipotesi in cui questo tipo di trattamenti è legittimo, si è reso necessario individuare una serie di garanzie ulteriori, di modo da assicurare quindi i diritti degli interessati in modo proporzionale al rischio cui sono esposti.

Considerata la diversa natura degli interessi in gioco, l'articolo in esame prevede che, nei casi in cui vi sia un presupposto contrattuale o consensuale, il titolare del trattamento debba comunque attuare «misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato [garantendo *n.d.a.*] almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione»[747]. Questi trattamenti poi – qualunque sia la base giuridica – non possono basarsi su particolari categorie di dati, a meno che non vi sia il consenso esplicito dell'interessato o il trattamento sia comunque necessario per motivi di interesse pubblico individuati *ex lege* dal diritto dell'Unione o degli Stati Membri; anche in questi casi, comunque, è necessario che siano previste «misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato».

Le questioni emerse circa l'esistenza o meno di un nuovo diritto ad una spiegazione degli algoritmi su cui lavorano i sistemi di *automatic decision-making* sono legate proprio a queste ultime previsioni[748]. Se infatti, in alcuni casi, la norma prevede che l'interessato abbia comunque il diritto di ottenere una revisione della decisione che lo interessa da parte di un operatore che (si presume) sia in grado di

---

[746] Reg. 679/2016, art. 22, § 2.

[747] *Ibidem*, art. 22, § 3.

[748] Celebre ormai il confronto che ha avuto spazio nel secondo numero del 2017 della rivista *International Privacy Data Law,* tra A. D. SELBST, J. POWLES, *Meaningful information and the right to explanation*, cit.; S. WACHTER, B. MITTELSTADT, L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, cit. Per maggiori approfondimenti, tuttavia, si rinvia alla vasta bibliografia citata in M.E. KAMINSKI, *The Right to Explanation, Explained*, in *Berkeley Technology Law Review*, 134/2019, pp. 189-218 (spec. nota n. 8).

verificare i risultati ottenuti dal sistema[749], da un punto di vista logico, per poter esercitare le prerogative che gli sono accordate, sembra necessario questi sia messo nelle condizioni di conoscere i criteri che guidano le operazioni, soprattutto quando intenda contestarne gli esiti o esprimere una propria opinione a riguardo.

Il testo del regolamento, tuttavia, in merito a questo punto risulta particolarmente ambiguo. Nonostante l'interessato abbia il diritto di conoscere dell'esistenza di questo tipo di procedimenti [750] e di ottenere «informazioni significative sulla logica utilizzata, nonché [sul]l'importanza e [sul]le conseguenze previste di tale trattamento»[751], nell'articolato non si rinviene alcun riferimento ad un vero e proprio diritto ad una spiegazione. È soltanto nei *considerando* (per l'esattezza al n. 71) che si accenna alla legittima pretesa «di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione»; una collocazione critica proprio per il valore giuridico non vincolante di queste statuizioni.

Alla luce di queste considerazioni, dunque, si è chiarito come la disciplina effettivamente imponga l'obbligo «di fornire informazioni significative sulla logica utilizzata, ma non necessariamente una spiegazione complessa degli algoritmi utilizzati o la divulgazione dell'algoritmo completo». Tuttavia, la complessità dei procedimenti non può essere utilizzata come pretesto per non fornire all'interessato indicazioni utili[752], così come non possono essere opposte in termini assoluti le prerogative legate alla protezione proprietà intellettuale e del segreto industriale[753]. Si è osservato che per garantire rimedi effettivi, è necessario che vengano fornite

---

[749] Un aspetto ritenuto *fondamentale* dalle Linee guida (cfr. Gruppo Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit. p. 30) rispetto al quale, si è arrivati ad individuare una sorta di principio alla "non esclusività" della decisione algoritmica (cfr. A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, cit., pp. 99-100).

[750] Reg. 679/2016, art. 13, § 2, lett. *f)* e art. 14, § 2, lett. *g*).

[751] *Ibidem*, art. 15, § 1, lett. *h).*

[752] *Ibidem*, *considerando 58*.

[753] *Ibidem*, *considerando 60 e 63.*

informazioni «sufficientemente complete affinché l'interessato possa comprendere i motivi alla base della decisione» e che vengano comunque individuate in ogni frangente idonee garanzie.

Chiarito dunque il portato della normativa europea, spetterà quindi ai legislatori nazionali, alle autorità di controllo e alla Corte di giustizia UE stabilire caso per caso quali siano le tutele più opportune rispetto all'utilizzo di questi trattamenti, suggerendo le soluzioni più consone per bilanciare gli interessi alla conoscibilità dei criteri decisionali con le contrapposte prerogative di segretezza[754].

### *5.4. Big data, big bias? L'esperienza italiana verso un utilizzo "costituzionalmente orientato" dei megadati e dell'AI*

Senza ombra di dubbio, l'utilizzo dei *big data* e del *machine learning* può dar luogo a distorsioni particolarmente serie e pregiudizievoli per le persone sottoposte a questo tipo di trattamenti. E ugualmente, rimane un punto fermo il fatto che gli interessati, per valere i propri diritti e contestare i risultati proposti dagli algoritmi, abbiano bisogno di conoscere le logiche con cui lavorano i programmi, così da poterne confutare i risultati.

Per affrontare con maggior contezza le questioni e le prospettive che si aprono a livello nazionale, però, per prima cosa è necessario approfondire la natura degli errori (*bias*) che possono intaccare questi sistemi, valutando poi, caso per caso, quali soluzione tecniche e giuridiche permettono di assicurare una miglior tutela alle persone coinvolte, senza pregiudicare eccessivamente gli interessi dei titolari del trattamento e dei proprietari delle licenze[755].

---

[754] A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e futuro delle libertà*, in *Rivista Biodiritto – BioLaw Journal*, n. 1/2019, p. 84.

[755] Come dimostrano gli scritti inizialmente proposti dalla dottrina in materia. Si vedano, *ex multis*, S. WACHTER, B. MITTELSTADT, C. RUSSELL, *Counterfactual explanations without opening the Black Box: automated decisions and the GDPR,* in Harvard Journal of Law & Technology 31(2), 2018, pp.

Come si diceva, da un punto di vista tecnico, si utilizza il termine *bias* per riferirsi «a sistemi informatici che discriminano sistematicamente e ingiustamente determinati individui o gruppi a favore di altri. Un sistema discrimina ingiustamente se nega un'opportunità o un bene o se assegna un risultato indesiderato ad un individuo o ad un gruppo di individui per motivi che sono irragionevoli o inappropriati»[756]. Esiti di questo tipo, peraltro, possono essere frutto di distorsioni di origine diversa, che possono interessare i dati con cui il sistema è stato testato, le logiche che ne orientano il funzionamento, piuttosto che il modo in cui l'utente utilizza questi strumenti o interpreta le informazioni che ottiene.

Il punto di partenza non potevano non essere gli errori legati alla qualità dei dati; un principio che, seppur fondamentale nell'ambito della *data protection*, risulta particolarmente ostico da garantire quando ci si trovi di fronte a *dataset* estesi come quelli legati ai *big data*. Si è avuto modo di osservare come i risultati proposti dagli algoritmi tendano a riflettere la qualità dei dati con cui sono stati allenati, secondo il principio che i *data scientists* hanno sintetizzato con l'espressione *garbage-in, garbage-out* (GIGO). In altri termini, se i contenuti utilizzati propongono una rappresentazione distorta di una certa realtà, il sistema tenderà a riproporre sistematicamente tali storture, anche perpetrando discriminazioni che dal punto di vista politico e sociale si vorrebbero debellare[757].

Approfondendo ulteriormente il problema, peraltro, si è colto come questo fenomeno – di per sé abbastanza intuitivo – sia dovuto in realtà ad errori ben diversi, legati ora alla qualità dei dati, in sé e per sé, ora alla loro qualificazione

---

842-887; A.J. KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H. YU, *Accountable Algorithms*, cit., M.E. KAMINSKI, *The Right to Explanation, Explained*, cit. (spec. pp. 217 ss.); G. MALGIERI, G. COMANDÉ, *Why a Right to Legibility of Automated Decisione-Making Exists in the General Data Protection Regulation*, in *International data Privacy Law*, 7(4), 2017, pp. 243-265.

[756] B. FRIEDMAN, H. NISSENBAUM, *Bias in Computer Systems*, in *ACM Transactions on Information Systems (TOIS)* 14/1996, pp. 330-347 come citati in A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, cit., pp. 96.

[757]

(un'operazione normalmente non automatizzata, che solleva quindi importanti questioni sul fronte delle responsabilità dei programmatori)[758].

A questo primo ordine di problemi, si aggiungono quelli legati alla programmazione dei sistemi; un aspetto che certo non è completamente scisso da quanto appena accennato rispetto ai dati, ma che merita una trattazione distinta.

Il regolamento infatti, in merito, non prevede alcunché di specifico (anche in nome del principio di neutralità tecnica), limitandosi solo a sottolineare come sia «opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate»[759]. Il tema evidentemente riguarda la conformità dei programmi rispetto ai fini perseguiti dal titolare, e interessa quindi tutti i profili relativi alla messa punto e all'utilizzo degli strumenti di cui questi si avvale[760]. Si possono così distinguere i c.d. *technical bias* – ossia quelli che «emergono come conseguenza di vincoli o decisioni tecniche. [E p]ossono trovarsi a livello grafico/visuale, di algoritmo o di input» – e i c.d. *emergent bias*, legati invece a come «l'uso di un software cambia nel tempo». Ad esempio «[a]ttraverso l'aggiunta di nuovi utenti, nuove fonti di dati, o per una molteplicità di altre possibilità, il *bias* può

---

[758] S. BAROCAS, A.D. SELBST, *Big Data's Disparate Impact*, in *California Law Review*, 104/2016, pp. 671-733 (spec. pp. 10-17, in merito ai problemi che si incontrano nella raccolta dei dati e nelle operazioni di *labeling*). Questo genere di errori vengono qualificati dalla letteratura scientifica come *pre-existing bias*, ossia storture «incorporati in un dato software perché l'organizzazione che ne determina i requisiti è *biased*» o, in alternativa, *bias* di misurazione, cioè «legati alla raccolta dei dati poi utilizzati nel *training* della macchina» (A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, cit., pp. 96).

[759] Reg. 679/2016, *considerando* 71, secondo periodo.

[760] Un tema, come già ricordato, particolarmente controverso nell'ambito della *data protection*, in quanto, sebbene il reg. 679/2016 preveda che il titolare adotti tutte le misure tecniche e organizzative necessarie a garantire la protezione dei dati *by design* e *by default* (art. 25), la normativa non prevede alcun obbligo per i produttori di tecnologie informatiche, accollando quindi all'utilizzatore tutte le responsabilità relative alla scelta della soluzione più opportuna. Sul punto si rinvia alle considerazioni espresse in B. VAN ALSENOY, *Data Protection Law in the EU: Roles, Responsibility and Liability*, cit., pp. .

emergere in modi che sarebbe stato difficile, se non impossibile, prevedere quando il sistema è stato costruito»[761].

Alla luce di queste considerazioni, dunque, si avverte chiaramente come la conoscibilità degli algoritmi (dei codici) di per sé possa rappresentare un punto di partenza, ma certo non la soluzione a questi problemi di discriminazione – in qualche modo – intrinseci al funzionamento dei sistemi in esame.

Per tale motivo, come accennato, a livello nazionale si è cominciato a guardare con favore non solo alla possibilità di riconoscere un vero e proprio diritto ad una spiegazione quanto anche (e soprattutto) alla possibilità di imporre specifiche garanzie per ottenere almeno una verifica controfattuale delle prestazioni degli algoritmi.

Sebbene i primi studi che hanno approfondito i diversi approcci adottati per implementare la normativa comunitaria mettano in luce come, su questi fronti[762], i legislatori statali nella maggior parte dei casi abbiano preferito adottare un impostazione negativa[763] (o comunque abbastanza neutra[764]) gli ordinamenti che –

---

761 A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, cit., pp. 96. Approfondendo il tema, però, possono registrarsi diversi tipi di alterazione – volontarie o involontarie – dovute innanzitutto a come sono impostati (e come si evolvono nel tempo) gli obiettivi che la macchina persegue (*target setting and variables*) e come quindi questa identifichi le diverse correlazioni all'interno dei *dataset* su cui lavora (dette anche operazioni di *clustering* e *class labeling*). E anche laddove si intervenga con specifiche limitazioni tecniche – volte, ad esempio, ad indentificare alcune caratteristiche rilevanti, così come a riequilibrare il peso di alcuni fattori (*proxy*) o ad escluderne altre (*masking*) – possono comunque verificarsi degli effetti indesiderati legati alle conseguenze di tali impostazioni (Cfr. S. BAROCAS, A.D. SELBST, *Big Data's Disparate Impact*, cit.).

762 G. MALGIERI, *Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations*, in *Computer Law and Security Review*, 2019 (disponibile *online* dal 9 luglio 2019).

763 La maggior parte degli Stati membri, infatti, pur avendo provveduto ad introdurre le debite misure di coordinamento dopo l'entrata in vigore del reg. 679/2016, non hanno comunque previsto *ex lege* alcuna nuova eccezione oltre a quelle previste a livello europeo (l'Italia, la Romania, la Svezia, la Danimarca, la Polonia, la Finlandia, Cipro, la Grecia, la Repubblica Ceca, l'Estonia, la Lituania, la Bulgaria, la Lettonia, il Portogallo, la Croazia, la Slovacchia, il Lussemburgo, Malta, e la Spagna). Per i riferimenti bibliografici si rimanda all'analisi proposta in G. MALGIERI, *Automated decision-making in the EU Member States*, cit., pp. 6-7.

soprattutto in ragione della loro cultura giuridica – hanno colto l'occasione per rinnovare il proprio sistema di tutele per restare al passo con lo sviluppo tecnologico, hanno introdotto ora nuove garanzie procedurali, ora dei veri e propri diritti. Paradigmatici, in tal senso, sono ad esempio gli obblighi di produrre una puntuale descrizione dei procedimenti e dei risultati, così come l'introduzione di particolari forme di *impact assessment* sugli algoritmi[765]. Allo stesso modo, è da accogliersi con particolare benevolenza la previsione di nuovi diritti alla conoscibilità dei pesi e dei parametri utilizzati dai diversi sistemi, così come della diversa funzione dei processi automatizzati nell'*iter* decisionale nel suo complesso[766].

Se queste sono le proposte maturate nell'ambito della disciplina sulla protezione dei dati personali, non vanno però trascurate le soluzioni che, attingendo da altri ambiti, possono comunque contribuire ad un significativo sviluppo del quadro delle garanzie per un *accountable automatic decision-making*. Ed è questo il caso dell'esperienza italiana, che nell'ambito della giurisprudenza amministrativa, ha cominciato a sviluppare una serie di principi volti ad assicurare un utilizzo "costituzionalmente orientato" dei sistemi di decisione automatizzata.

I tribunali regionali così come il Consiglio di stato, infatti, negli ultimi anni hanno avuto occasione di tornare a più riprese su questi temi, chiarendo come, anche qualora l'attività dei pubblici funzionari e degli uffici venga sostituita da nuovi

---

[764] È questo il caso di Germania e (in parte) dell'Austria, che hanno provveduto all'implementazione dell'art. 22 reg. 679/2016 nella propria legislazione nazionale ma senza prevedere alcuna specifica e ulteriore garanzia a tutela della persona interessata. G. MALGIERI, *Automated decision-making in the EU Member States*, cit..

[765] In tal senso fan scuola le esperienze di Regno Unito, Slovacchia e Irlanda, in cui sono stati introdotti, ad esempio particolari obblighi informativi (includendo anche accurate descrizioni dei meccanismi decisionali) o alcune forme di valutazione di impatto sugli algoritmi. G. MALGIERI, *Automated decision-making in the EU Member States*, cit.

[766] Sono gli esempi che si rinvengono in Francia e in Ungheria dove è stato introdotto un diritto a conoscere il peso che i diversi parametri assumono nei singoli passaggi del processo decisionale. G. MALGIERI, *Automated decision-making in the EU Member States*, cit.

sistemi automatizzati, non possono di fatto venir meno le garanzie che discendono da quanto previsto dalla nostra Carta fondamentale[767].

È interessante notare come, nel tempo, questo filone giurisprudenziale abbia a messo in luce due profili, l'uno complementare all'altro, concentrandosi, da un lato, sul diritto di difesa e di non discriminazione (*ex* artt. 24 e 3 Cost.) e, all'opposto, sui principi di buon andamento della pubblica amministrazione di cui all'art. 97 Cost.

Dovendo qualificare l'attività dei sistemi in esame all'interno dell'attività della pubblica amministrazione, infatti, i giudici amministrativi dapprima hanno messo in luce come se un algoritmo, nella sostanza, gestisce in modo automatico e per mezzo di un complesso sistema informatico il procedimento, in qualche modo, questo finisce per sostituire esso stesso il procedimento medesimo, divenendo «diretta espressione dell'attività svolta dalla pubblica amministrazione che è indubbiamente attività di pubblico interesse»[768].

Alla luce di queste considerazioni, dunque, in altra sede, lo stesso Tribunale è giunto a concludere che «non è conforme al vigente plesso normativo complessivo e ai dettami dell'art. 97 della Costituzione ai principi ad esso sottesi agli istituti di partecipazione procedimentale definiti agli artt. 7, 8, 10 e 10 – bis della L. 7/8/1990, n. 241, all'obbligo di motivazione dei provvedimenti amministrativi sancito dall'art. 3, stessa legge, al principio ineludibile dell'interlocuzione personale intessuto nell'art. 6 della legge sul procedimento e a quello ad esso presupposto di istituzione della

[767] I riferimenti sono soprattutto alle pronunce del TAR Lazio, sez. III bis, sentt. n. 3769/2017 e 9224-9230/2018, nonché dalla recentissima decisione del Consiglio di Stato, sez. VI, sent. n. 2270/2019. In tutti e tre i casi, oggetto di censura era quanto previsto dalla legge n. 107/2015 che autorizzato il Ministero dell'Istruzione, dell'Università e della Ricerca ad attuare un piano straordinario di assunzioni a tempo indeterminato di personale docente per le istituzioni scolastiche di ogni ordine e grado. Tale normativa, nello specifico, aveva previsto che l'intera procedura di assegnazione dovesse essere gestita da un sistema informatico che avrebbe provveduto automaticamente all'assegnazione delle sede, secondo i criteri stabili dalla legislazione vigente. A queste peraltro sono seguite una lunga serie di pronunce, anche di fronte ai giudici ordinari, che in linea con quanto si dirà a breve hanno progressivamente consolidato un orientamento garantista.

[768] TAR Lazio, sez. III bis, sent. n. 3769/2017, § 2.

figura del responsabile del procedimento, affidare all'attivazione di meccanismi e sistemi informatici e al conseguente loro impersonale funzionamento, il dipanarsi di procedimenti amministrativi»[769]. Constatando come questi sistemi, alla stregua dell'attività dei pubblici uffici, siano in grado di incidere su interessi e diritti di rilevanza costituzionale, il Collegio osserva infatti «che le procedure informatiche, finanche ove pervengano al loro maggior grado di precisione e addirittura alla perfezione, *non possano mai soppiantare, sostituendola davvero appieno, l'attività cognitiva, acquisitiva e di giudizio che solo un'istruttoria affidata ad un funzionario persona fisica è in grado di svolgere* […] ostando alla deleteria prospettiva orwelliana di dismissione delle redini della funzione istruttoria e di abdicazione a quella provvedimentale, il presidio costituito dal baluardo dei valori costituzionali scolpiti negli artt. 3, 24, 97 della Costituzione oltre che all'art. 6 della Convezione europea dei diritti dell'uomo»[770].

Simili considerazioni, da ultimo hanno trovato ulteriori argomenti in quanto disposto nell'aprile 2019 dal Consiglio di Stato, il quale, al termine di questa complessa *querelle* giudiziaria, ha osservato come se, da un lato, «l'assenza di intervento umano in un'attività di mera classificazione automatica dei istanze numerose, secondo regole predeterminate (che sono, queste sì, elaborate dall'uomo), e l'affidamento di tale attività a un efficiente elaboratore elettronico appaiono come doverose declinazioni dell'art. 97 Cost. coerenti con l'attuale evoluzione tecnologica»[771], dall'altro, «l'utilizzo di procedure "robotizzate" non può, tuttavia, essere motivo di elusione dei principi che conformano il nostro ordinamento e che regolano lo svolgersi dell'attività amministrativa»[772]. Considerando quindi il *software* come un "atto amministrativo informatico", «la regola algoritmica deve essere non

---

[769] TAR Lazio, sez. III bis, sent. n. 9224-9230/2018, § 5.

[770] *Ibidem*, § 5.1.

[771] Cons. di Stato, sez. VI, sent. n. 2270/2019, § 8.1. Una conclusione, questa, che porterebbe ad escludere la possibilità – anche solo in astratto – di ipotizzare l'utilizzo di forme di *unsupervised machine learning* di apprendimento progressivo e di *deep learning* nell'ambito delle attività della pubblica amministrazione (*ibidem*, § 8.2).

[772] *Ibidem*, § 8.2.

solo conoscibile in sé, ma anche soggetta alla piena cognizione, e al pieno sindacato, del giudice amministrativo»[773], poiché «solo in questo modo è possibile svolgere, anche in sede giurisdizionale, una valutazione piena della legittimità della decisione» [774] vagliando il rispetto dei principi di imparzialità, pubblicità e trasparenza.

Chiaramente, in questi casi, le questioni legate alla tutela della proprietà intellettuale del programma, sono stati agilmente ovviate. Già nelle loro prime pronunce, infatti, i giudici amministrativi avevano avuto modo di constatare come nel momento in cui l'«algoritmo è entrato nella procedura quale elemento decisivo e lo stesso è, comunque, stabilmente detenuto dalla stessa amministrazione ministeriale che lo ha commissionato» gli interessi di carattere pubblico connessi alla trasparenza e all'imparzialità della procedura prevalgono su quelli di natura proprietaria legati alla programmazione del *software*, poiché risultano essi stessi in capo ai medesimi uffici.

Probabilmente, in altri frangenti – come, ad esempio, nei rapporti tra privati o nel caso in cui gli algoritmi fossero semplicemente in concessi dotazione della p.a. – gli esiti potrebbero essere diversi. Il completo disvelamento delle logiche utilizzate dai sistemi, infatti, potrebbero comportare un importate pregiudizio in capo a quanti hanno investito nel loro sviluppo; ragion per cui sarebbe più opportuno valutare altri rimedi.

Alla luce del quadro tracciato, tuttavia, emerge come l'intento di preservare i valori propri del costituzionalismo italiano ed europeo stiano fungendo da potente propulsore nell'aggiornamento del sistema di garanzie rispetto al mondo dei *big data*. Certamente, il linguaggio dei diritti contribuisce alla messa a punto di soluzioni tese a determinare il più equo bilanciamento degli interessi che si contrappongono in quest'ambito e si auspica che questo possa valere anche a fronte dei forti poteri

[773] *Ibidem*, § 8.4.
[774] *Ibidem*.

economici e informativi che oggi connotano i grandi attori di mercato. In particolare, ancorando le garanzie legate alla protezione dei dati personali ai principi procedurali e sostanziali ereditati dalla tradizione (trasparenza, non discriminazione, pluralismo in testa) queste possono contribuire all'emergere non solo di nuove soluzioni tecniche – come le valutazioni di impatto o la conoscibilità dei criteri di ponderazione delle decisioni – ma anche ad una rilettura costantemente aggiornata dei diritti fondamentali, avendo cura non solo del diritto di difesa, ma anche delle altre libertà che connotano una società autenticamente democratica.

# Conclusioni

## Il costituzionalismo tecnologico europeo: quali prospettive?

Al termine di questo lavoro, avendo a mente la domanda con da cui si era cominciato, si possono trarre alcune osservazioni conclusive (sebbene, per forza di cose, non definitive).

Il quesito di ricerca apriva alla riflessione sulla funzione costituzionale del diritto alla protezione dei dati personali, focalizzando l'attenzione soprattutto sul rapporto tra l'ordinamento costituzionale nazionale e il sistema giuridico europeo nell'elaborazione della relativa disciplina per quanto concerne la realtà dei *big data*.

Partendo dal considerare lo stato dell'arte all'interno dell'esperienza giuridica italiana, si è avuto modo di osservare, innanzitutto, come il Giudice delle leggi negli anni abbia avuto poche occasioni per pronunciarsi precipuamente su questi temi. La giurisprudenza, infatti, nel tempo si è concentrata soprattutto sull'opportunità di estendere copertura costituzionale a nuovi diritti sostanziali come la riservatezza o l'identità personale, affrontando solo incidentalmente le questioni relative alla protezione dei dati personali.

Proseguendo, si è osservato, come l'elaborazione di una disciplina in quest'ambito – in particolare, nel contesto italiano – si debba soprattutto al processo di integrazione europea. È grazie all'esigenza di promuovere la libera circolazione dei servizi e dei cittadini che si è arrivati all'approvazione della dir. 95/46 e, sempre in quest'ottica, si è gradualmente promosso il completamento della prima strategia comunitaria in materia di *data protection*.

Si è visto, in particolare, come questa normativa intercetti diversi interessi e, sul piano del diritto costituzionale, rappresenti una sorta di trasposizione in chiave informativa delle tradizionali garanzie a tutela dei diritti fondamentale e della *rule of law*. Formalmente, essa si connota dunque come una regolamentazione di tipo procedurale, volta ad individuare la regola e le eccezioni con cui addivenire , di volta in volta, al necessario contemperamento degli interessi legati al trattamento dei dati in ciascun contesto.

Nonostante queste forti connessioni con gli studi e le questioni di diritto costituzionale, tuttavia, soltanto alcuni Stati hanno provveduto ad emendare le proprie Carte fondamentali per far spazio a questo nuovo diritto, spesso rimettendo questo compito alle Corti di vertice perché intervenissero con la loro giurisprudenza.

In tal senso, dunque, al tempo, è stata accolta con una certa sorpresa la scelta di introdurre un nuovo diritto fondamentale europeo alla protezione dei dati personali, a sé stante e autonomo rispetto alle tradizionali garanzie che l'avevano sempre letto con sistema di garanzie strumentale alla *privacy*. E allo stesso modo, in seguito a questa prima novità, solleva ancora qualche interrogativo l'effettiva portata delle competenze europee in quest'ambito, così come riformate nel *post*-Lisbona dall'art. 16 TFUE.

Se infatti oggi, grazie a questi riferimenti "costituzionali" europei, le strategie di *data-governance* trovano la loro sede di elezione in Bruxelles – peraltro sempre più spesso attraverso atti-fonte di immediata applicazione, come i regolamenti – la molteplicità di interessi che si intersecano in questa materia rendere difficile inquadrare il ruolo costituzionale di quanto sancito dall'art. 8 CDFUE, così come i rapporti che legano questo nuovo diritto con gli altri tutelati dalla Carta e delle Costituzioni nazionali.

Com'è emerso analizzando la nuova "pietra miliare" di questa disciplina – il reg. 679/2016 – se a livello europeo possono essere individuate figure e meccanismi

di tutela sempre più all'avanguardia e al passo come le nuove tecnologie, nel momento in cui si pretende di attrarre nell'orbita della *data protection* ogni questione che, in qualche modo, abbia a che fare con i dati, la situazione diventa problematica.

Nel delinearsi di questo nuovo sistema, in particolare, risulta critico il ruolo che va assumendo la Corte di giustizia, facendo dei giudici europei l'ultima voce legittimata a pronunciarsi ogni qual volta vengano ad essere toccati questi temi. Interlocutore privilegiato per ogni questione riguardi la corretta interpretazione del diritto dell'Unione, il Collegio lussemburghese, dimostra una certa propensione per una lettura estensiva non solo della portata disciplina e dei suoi presupposti, ma anche delle proprie competenze. E così, in questo modo, bilanciamenti di interessi prima spettanti al legislatore e ai giudici nazionali, sono progressivamente attratti "verso l'alto", in sede europea, in una progressiva esautorazione delle Corti costituzionali nei confronti delle questioni inerenti di diritti fondamentali legati ai dati.

Tutto ciò solleva non poche perplessità. Accentrando a Bruxelles la competenza legislativa e a Lussemburgo quella giudiziaria per ogni questione riguardi la protezione dei dati personali, si tende ad un irrigidimento del sistema, senza contare le profonde differenze che oggi esistono tra i diritti fondamentali garantiti a livello comunitario e quelli invece tutelati dalle Carte nazionali. Come si è avuto modo di osservare, infatti, pur contribuendo alla definizione di una *digital rule of law* europea, la Corte di giustizia si dimostra incline a bilanciamenti tra *privacy* e *data protection* ben diversi da quelli che invece potrebbero prediligere le Corti nazionali. E lo stesso può dirsi per quanto riguarda i contemperamenti delle prerogative legate ai diritti contrapposti alla tutela della vita privata, spesso sacrificati in nome di un interpretazione individualistica del *bill of rights* europeo.

Nel contrastare questi chiaro-scuri del c.d. *effetto Bruxelles*[775], sono quindi da guardare con particolare interesse i tentativi di dialogo inter-istituzionale che già si registrano nelle prime fasi di attuazione del GDPR, così come le iniziative intraprese da alcuni Stati per promuovere un approccio più specifico e garantista nei confronti delle tecnologie *data-intensive*.

È attraverso questi canali che potranno crearsi nuovi margini di confronto sulle questioni legate allo sviluppo di un costituzionalismo tecnologico europeo. Se, infatti, il legislatore nazionale saprà sfruttare i margini di discrezionalità concessigli dalla disciplina comunitaria, gli accorgimenti e le tutele promosse in un contesto potranno presto ispirare le linee interpretative che guidano l'applicazione della normativa generale, così come la giurisprudenza europea. Allo stesso modo, gli studi attualmente condotti a livello nazionale per far fronte ai problemi che si incontrano nell'utilizzo dell'intelligenza artificiale e del *machine learning* potranno contribuire alla definizione di una disciplina comune sul tema, spostando così l'attenzione dagli aspetti etici a quelli più propriamente giuridici[776].

Si tratterà senz'altro di un percorso graduale, rispetto al quale servirà tempo e pazienza. Cionondimeno, la pretesa di un dialogo rispetto alla definizione delle

---

[775] È ormai d'uso parlare del c.d. «effetto Bruxelles» (*Brussels Effect*) identificando in questi termini la capacità dimostrata dall'Unione europea di promuovere ed esportare i propri standard senza passare per le strettoie legate ai metodi che tradizionalmente contraddistinguono il diritto internazionale. Tutto ciò si verifica non solo nel campo della protezione dei dati personali, ma anche in altre materie come, ad esempio, nell'ambito della disciplina sulla concorrenza e sulla sicurezza alimentare, creando particolari tensioni soprattutto nei rapporti con il mercato nord americano. Cfr. A. BRADFORD, *The Brussels Effect*, in *Columbia Law Rewiew*, 107, 2012.

[776] Agenzia europea per i diritti fondamentali (FRA), *Fundamental Rights Report 2019 – Information society, privacy and data protection* (sezione n. 7), 6 giugno 2019, p. 157. Si osserva, infatti, «by the end of 2018, Member States had understood the significant impact that artificial intelligence can have on industry and the labor market. The solutions to ease this technological transition – focusing on increased research and resources – are well under way within most Member States. Foreseeing the economic and labor impacts that AI may have on individuals is necessary to ensure the cohesion of society. However, Member States should also pay close attention to the impact that AI will have on fundamental rights, and should prepare adequate strategies to ensure that such rights, and not only ethical considerations, will be duly respected.»

funzioni costituzionali del diritto alla protezione dei dati personali, in ambito nazionale così come europeo, si pone come uno passaggio ineludibile, da cui dipende in larga parte anche il successo della stessa strategia comunitaria in questo settore.

Rispetto ai delicati equilibri sottesi a questa materia, si sono già riscontrate non poche tensioni, e queste potrebbero registrare sensibili evoluzioni se si considera il nuovo ruolo dei giudici europei quali garanti costituzionali dei diritti digitali. Come documentano i rinvii pregiudiziali, così come alcune pronunce delle Corti di vertice nazionale, i potenziali conflitti relativi alle reciproche competenze e ai criteri di giudizio rispetto a questi temi sono tutt'altro che appianati.

Se infatti il Collegio del Lussemburgo non sembra disposto a transigere sulle proprie competenze – neanche quando nel frattempo sulle medesime questioni si sia già venuta a pronunciare i giudici costituzionali[777] – al contempo non tutte le Corti sembrano propense a dare pacifica prevalenza al sindacato europeo nelle questioni che presentino il rischio di una sovrapposizione pregiudizievole ai valori costituzionali interni.

Il riferimento è chiaramente al drastico cambio di orientamento che si è registrato negli ultimi anni, soprattutto nella giurisprudenza costituzionale italiana: una serie di evoluzioni certamente non concluse (ed anzi, apertamente *in divenire*), ma che già hanno avuto modo di soffermarsi proprio sulle questioni relative al rapporto tra *dati* e *diritti*[778].

---

[777] CGUE, sent. 20 dicembre 2017, *Global Starnet Ltd c. Ministero dell'Economia e delle Finanze e Amministrazione Autonoma Monopoli di Stato* (causa C-322/16); in cui si legge che «il fatto che la Corte costituzionale italiana si sia pronunciata sulla conformità delle disposizioni del diritto nazionale, costituenti anche l'oggetto della seconda questione pregiudiziale, alle disposizioni della Costituzione italiana che il giudice del rinvio considera, in sostanza, come le norme di riferimento corrispondenti e identiche agli articoli 26, 49, 56 e 63 TFUE e all'articolo 16 della Carta dei diritti fondamentali, non ha alcuna incidenza sull'obbligo, previsto dall'articolo 267 TFUE, di sottoporre alla Corte eventuali questioni riguardanti l'interpretazione del diritto dell'Unione» (§ 25).

[778] Corte cost. sent. n. 20 del 2019.

Sebbene si tratti di conflitti più legati alla convergenza degli strumenti di tutela, piuttosto che alla loro divergenza, non si può fare a meno di avvertire come, anche in Italia, il Giudice delle leggi avverta l'esigenza di un nuovo confronto sui criteri con cui le questioni relative ai diritti fondamentali possono essere decise, senza più spogliarsi anzitempo delle sue prerogative.

Disposti anche a dei «visibili e significativi scostamenti dai canoni che stanno a base dello svolgimento dei giudizi di costituzionalità»[779] i giudici della Consulta pur non cercando lo scontro con i colleghi europei, dimostrano come, anche su questi fronti sia loro intenzione continuare mantenere la loro competenza più importante, ossia quella di proteggere il nucleo intangibile di valori sui quali si fonda il nostro ordinamento costituzionale. E questo non solo per i diritti coincidenti, ma anche per quei valori che, pur riconducibili principalmente alla Carta di Nizza e al diritto europeo, trovano comunque validi riferimenti all'interno del dettato costituzionale interno.

E questi orientamenti sembrano, peraltro, quanto mai decisi a consolidarsi, e dunque dipenderà dal proficuo dialogo che andrà ad istaurarsi tra le diverse corti di vertice le possibilità di veder affermato appieno il potenziale del *digital constitutionalism* europeo.

Quest'ultimo accenno, in particolare, merita scrupolosa attenzione. Se, come suggerito da alcuni, il diritto europeo ha contributo a dare vita a nuove Costituzioni, poliedriche e molteplici tanti sono i campi in cui si spiegano le competenze comunitarie[780], non può passare in secondo piano il ruolo svolto Bruxelles nel delinearsi di una nuova forma di costituzionalismo tecnologico europeo.

---

779 A. RUGGERI, *La Consulta rimette a punto di i rapporti tra diritto eurounitario e diritto interno con una pronunzia in chiaro scuro (A prima lettura i Corte cost. nt. n. 20 del 2019)*, in *Consulta Online*, 25 febbraio 2019, pp. 113-114-

780 K. TOURI, *The Many Constitutions of Europe*, in K. TOURI, S. SANKARI (a cura di), *The Many Constitutions of Europe*, New York, Routlege, 2016 (capitolo 1).

Come dimostrano, infatti, l'evoluzione del quadro normativo sulla protezione dei dati personali e le iniziative ora promosse per affrontare le questioni etico-giuridiche connesse allo sviluppo dell'Ai, l'Unione europea, nei limiti del possibile, in questi ambiti si afferma come un attore autorevole, all'altezza delle sfide che su questi temi dovranno essere affrontate a livello globale.

Cionondimeno, questa posizione di forza, non può essere sfruttata senza le debite attenzioni a quello che il contesto interno di questa realtà sovranazionale, e così la pluralità di esperienze e culture giuridiche da cui questo nuovo costituzionalismo attinge. Se, come ormai evidente, negli ultimi anni, il processo di integrazione comunitaria vive un momento di crisi, in cui continuamente si tenta di prevenire lo sfaldamento e di curare la tenuta del fondamento valoriale comune[781], il «problema costituzionale» deve essere affrontato secondo logiche dialettiche e partecipative.

Il tempo darà ragione rispetto a queste prospettive, soprattutto via via che verranno a definirsi le questioni ora pendenti di fronte alla CGUE, sull'applicazione del reg. 679/2016 così come degli altri atti che concorrono alla *data governance* europea. Quel che è certo è che, considerate le reazioni delle Corti costituzionali nel passato più o meno recente, la protezione dei dati diventerà un tema sempre più centrale in questo confronto costituzionale europeo, punto di partenza per ogni futura riflessione sulla tutela dei diritti fondamentali al tempo dei *big data*.

[781] Parafrasando qui le parole di Giuliano Amato, in ID., *L'integrazione europea come problema costituzionale*, in *Quaderni Costituzionali*, n. 3/2018, p. 563.

Bibliografia


AA.VV., *La nascita delle Costituzioni europee del secondo dopoguerra*, Associazione Italiana dei Costituzionalisti, Padova, Cedam, 2000

ADAM R., TIZZANO A., *Manuale di diritto dell'Unione europea,* Torino, Giappichelli, 2017

AGID, *L'intelligenza artificiale al servizio del cittadino: sfide e opportunità*, marzo 2018

ALBERS M., *Realizing the Complexity of Data Protection*, in S. GUTWIRTH, R. LEENES, P. DE HERT (a cura di), *Reloading data protection. Multidisciplinary Insights and Contemporary Challenges*, Dordrecht, Springer, 2014

ALPA G., BESSONE M., BONESCHI L. (a cura di), *Il diritto all'identità personale*, Padova, Cedam, 1981.

ALPA G., *Privacy e statuto dell'informazione (il* privacy act 1974 *e* la Loi relative à l'informatique, aux fichiers at aux libertés *n. 78.17 del 1978)*, in M. BESSONE, G. GIACOBBE (a cura di), *Il diritto alla riservatezza in Italia e ed in Francia,* Padova, Cedam, 1988

AMATO G., *L'integrazione europea come problema costituzionale*, in *Quaderni Costituzionali*, n. 3/2018

ARENA L., *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?* in *Quaderni Costituzionali*, 2014

AVITABILE A., *Il* Data Protection Officer*,* in G. FINOCCHIARO (diretto da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017

AZZENA L., *Prospettive della Carta europea dei diritti e ruolo della giurisprudenza*, in G.F. FERRARI (a cura di), *I diritti fondamentali dopo la Carta di Nizza. Il costituzionalismo dei diritti*, Milano, Giuffrè, 2001

BALDASSARRE A., *Privacy e Costituzione. L'esperienza statunitense*, Roma, Bulzoni Editore, 1975

BARBERA A., *"Nuovi diritti": attenzione ai confini¸* in L. CALIFANO (a cura di), *Corte costituzionale e diritti fondamentali¸* Torino, Giappichelli, 2004

BARBERA A., *I principi costituzionali della libertà personale*, Milano, Giuffrè, 1967

BARBERA A., *Principi fondamentali. Articolo 2*, in G. BRANCA (a cura di), *Commentario alla Costituzione*, Bologna-Roma, Zanichelli, 1975

BAROCAS S., A.D. SELBST, *Big Data's Disparate Impact*, in *California Law Review*, 104/2016, pp. 671-733

BARONE A., *Il diritto del rischio*, Milano, Giuffrè, 2006

BASSINI F., TIBERI G. (a cura di), *La Costituzione europea. Un primo commento*, Bologna, Il Mulino, 2004

BASSINI F., TIBERI G. (a cura di), *Le nuove istituzioni europee. Commento al Trattato di Lisbona*, Bologna, Il Mulino, 2008

BASSINI F., TIBERI G. (a cura di), *Una Costituzione per l'Europa. Dalla Convenzione europea alla Conferenza intergovernativa*, Bologna, Il Mulino, 2003

BASSINI M., *Google davanti alla Corte di giustizia: il diritto all'oblio*, in *Quaderni costituzionali*, n. 3, 2014, pp. 730-733

BENNETT C.J., *Regulating Privacy. Data Protection and Public Policy in Europe and the United States,* Ithaca-Londra, Cornell University Press, 1992

BIFULCO R., CARTABIA M., CELOTTO A., *Introduzione,* in IID. (a cura di), *L'Europa dei diritti*, Bologna, Il Mulino, 2001

BIGNAMI F, *Protecting Privacy Against the Police in the European Unione: The Data Retention Directive*, in Y. BOT (a cura di), *Melanges en l'Honneur de Philippe Leger: le droit a mesure de l'homme*, Parigi, 2006

BIGNAMI F., *Privacy and Law Enforcement in the European Unione: The Data Retention Directive*, in *Chicago Journal of International Law*, 2007, pp. 233-255

BILOTTA F., *L'emersione del diritto alla privacy*, in A. CLEMENTE (a cura di), *Privacy*, Padova, Cedam, 1999

BIN R., CARETTI P., PITRUZZELLA G., *Profili costituzionali dell'Unione europea*, Bologna Il Mulino, 2015

BIN R., *Diritti e argomenti: il bilanciamento degli interessi nella giurisprudenza costituzionale*, Milano, Giuffrè, 1992

BIN R., PITRUZZELLA G., *Diritto Pubblico*, Torino, Giappichelli, 2017

BIN R., *Taricco, una sentenza sbagliata: come venirne fuori?*, in A. BERNARDI (a cura di), *I controlimiti. Primato delle norme europee e difesa dei principi costituzionali*, Napoli, Jovene, 2017

BING J., *A Comparative Outline of Privacy Legislation*, in *Comparative Law Yearbook*, 2, 1978

BOLLIER D., *The Promise and Perils of Big Data* Aspen Institute, Communications and Society program, 2010

BOLOGNINI L., PELINO E., BISTOLFI C., *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè, 2016

BÖRÖCZ I., *Risk to the Right to Protection of Personal Data*, in *European Data Protection Law Review*, 4, 2016, pp. 467-480

BOZZI L., *Il diritto di conoscere le proprie origini*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019

BRADFORD A., *The Brussels Effect*, in *Columbia Law Review*, 107, 2012, pp. 1-68

BRAVO F., *Il consenso e le altre condizioni di liceità del trattamento dei dati personali*, in G. FINOCCHIARO (diretto da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017

BRAVO F., *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. CUFFARO, R. D'ORAZIONE, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019

BROWN I., *Online Freedom of Expression, Assembly, Association and the Media in Europe,* pubblicato *online* in seguito alla *Council of Europe Conference of Ministers on Freedom of Expression and Democracy in the Digital Age*, MCM(2013)007

BROWNSWORD R., *So What Does the World Need Now? Reflections on Regulating Technologies*, in R. BROWNSWORD, K. YEUNG (a cura di) *Regulating technology*, Oxford, Hart Publishing, 2008,

BUTTARELLI G., *Banche dati e tutela della riservatezza. La* privacy *nella Società dell'Informazione*, Milano, Giuffrè, 1997

BUTTARELLI G., *What Future for the Data Retention Directive*, Gruppo Articolo 29

BUTTURINI D., *La tutela dei diritti fondamentali nell'ordinamento costituzionale italiano ed europeo*, Napoli, Editoriale Scientifica Italiana, 2009

BYGRAVE L.A., *Automated profiling – Minding the machine: article 15 of EC Data Protection Directive and Automated Profiling*, in *Computer Law and Security Review*, 17, 2001, pp. 17-24

BYGRAVE L.A., *Data Protection Law – Approaching Its Rationale, Logic and Limits*, L'Aia-Londra-New York, Kluwer Law International, 2002

BYGRAVE L.A., SCHARTUM D., *Consent, Proportionality and Collective Power*, in S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE, S. NOUWT (a cura di), *Reinventing Data Protection?,* Dordrecht, Springer, 2009

CALIFANO L., COLAPIETRO C., *Introduzione*, in ID. (a cura di), *Innovazione tecnologica e valore della persona*, Napoli, Editoriale Scientifica, 2017

CALIFANO L., *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2017

CALIFANO L., *Privacy: Affermazione e pratica di un diritto fondamentale*, Napoli, Editoriale Scientifica, 2016

CALZOLAIO S. *Protezione dei dati personali*, in *Digesto delle discipline pubblicistiche*, Torino, Utet, 2017 (edizione *online*)

CALZOLAIO S., FEROLA L., FIORILLO V., ROSSI E.A., TIMIANI M., *La responsabilità e la sicurezza del trattamento*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2017

CANNIZZARO A., *Sistemi concorrenti di tutela dei diritti fondamentali e controlimiti costituzionali*, in A. BERNARDI (a cura di), *I controlimiti. Primato delle norme europee e difesa dei principi costituzionali*, Napoli, Jovene, 2017

CAPALDO E., *Riservatezza, vita privata e tutela della dignità del lavoratore "agile"*, in *Giustiziacivile.com*, 2018

CAPOTOSTI P.A., *La Corte costituzionale: giudice delle libertà o dei conflitti?*, in B. CARAVITA (a cura di), *La giustizia costituzionale in trasformazione: la Corte costituzionale tra giudice dei diritti e giudice dei conflitti*, Jovene, Napoli, 2012

CARTABIA M., *Art. 51 Ambito di applicazione*, in BIFULCO R., CARTABIA M., CELOTTO A., *Introduzione,* in IID. (a cura di), *L'Europa dei diritti*, Bologna, Il Mulino, 2001

CARTABIA M., *L'ora dei diritti fondamentali nell'Unione europea*, in EAD. (a cura di), *I diritti in azione*, Bologna, Il Mulino, 2007

CARTABIA M., *Le norme sulla privacy come osservatorio sulle tendenze attuali delle fonti del diritto*, in M. LOSANO (a cura di), *La legge italiana sulla* privacy, Roma, Laterza, 2001

CARTABIA M., *Principi involabili e integrazione europea*, Milano, Giuffrè, 1995

CARUSO C., *La Corte costituzionale riprende il cammino comunitario: invito alla discussione sulla sentenza n. 269 del 2017*, in *Forum di Quaderni Costituzionali*, 18 dicembre 2017

CASINI M., CASINI C., *Il dibattito sulla PMA eterologa all'indomani della sentenza costituzionale n. 162 del 2014. In particolare: il diritto a conoscere le proprie origini e l'"adozione per la nascita"* in *Rivista di Biodiritto,* 2, 2014, pp. 135-155

CASSANO G., AQUINO M., *Il trattamento dei dati personali alla luce della direttiva 2002/58,* in *I Contratti*, 2003, pp. 402-412

CERRI A., *Diritto di non ascoltare l'altrui propaganda*, in *Giurisprudenza Costituzionale*, I, 1985, pp. 987-991

CERRI A., *La costituzione e il diritto privato*, in P. RESCIGNO (dir.), *Trattato di diritto privato*, vol. I., Torino, Utet, 1999

CERRI A., *Libertà negativa di manifestazione del pensiero e di comunicazione privata. Diritto alla riservatezza: fondamenti e limiti*, in *Giurisprudenza Costituzionale*, I, 1974, pp. 610-615

CERRI A., *Riservatezza*, in *Enciclopedia giuridica*, vol. XXVII, Istituto della Enciclopedia Italiana, Roma, 1995

CHANDER A., *Facebookistan*, 90 *North Carolina Law Review*, 2012, pp. 1808-1844.

CHESSA O., *Meglio tardi che mai. La dogmatica dei controlimiti e il caso Taricco*, in A. BERNARDI (a cura di), *I controlimiti. Primato delle norme europee e difesa dei principi costituzionali*, Napoli, Jovene, 2017

CHOWDHURY N.*, I, Spy (But Only On You):* Raza v City of New York*, The Civil Rights Disaster of Religious and Ethnic- Based Surveillance and the National Security Excuse,* in *Columbia Human Rights Law Review,* 2014-15, pp. 278-331

CLARKE R., *Introduction to Dataveillance and Information Privacy, and Definitions of Terms* (disponibile *online*)

CLEMENTI F., *La Convenzione sull'avvenire dell'Europa: il mandato, l'organizzazione, i lavori*, in F. BASSINI, G. TIBERI (a cura di), *Una Costituzione per l'Europa. Dalla Convenzione europea alla Conferenza intergovernativa*, Bologna, Il Mulino, 2003

COCQ C. - GALLI F., *Comparative law paper on data retention regulation in sample of EU Member States*, 2013, pp. 1-32

COLAPIETRO C., IANNUZZI A., *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2017

COLAPIETRO C., IANNUZZI A.*, Il cammino della trasparenza in Italia: una prospettiva di partecipazione e legittimazione*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Napoli, Editoriale Scientifica, 2014

COLAPIETRO C., *Tutela della dignità e riservatezza del lavoratore nell'uso delle tecnologie dei digitali per finalità di lavoro,* in *Giornale di diritto del lavoro e delle relazioni industriali,* 2017, pp. 439-469

COSTANZO P., *I diritti nelle "maglie" della Rete*, in L. BRUSCAGLIA, R. ROMBOLI, *Diritto pubblico e diritto privato nella rete delle nuove tecnologie*, Pisa, 2010

COSTANZO P., MEZZETTI L., RUGGERI A. *Lineamenti diritto costituzionale dell'Unione europea*, Torino, Giappichelli, 2014

CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *Il codice del trattamento dei dati personali*, Torino, Giappichelli, 2007

CUFFARO V., *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019

CUFFARO V., *Quel che resta di un codice: il D.lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del Codice della Privacy al Regolamento sulla protezione dei dati*, in *Corriere giuridico*, n. 10, 2018, pp. 1181-1185

D'ACQUISTO G., M. NALDI, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, Giappichelli, 2017

D'ALOIA A. (a cura di), *Biotecnologie e valori costituzionali*, Torino, Giappichelli, 2005

D'ALOIA A., *L'(ex) 40*, in *Quaderni costituzionali*, 4, 2015, pp. 997-999

D'ORAZIO R., *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019

DALY A., A. CARLON, T. VAN GEELEN, *Data and fundamental rights*, in V. MAK, E. TJONG TJIN TAI, A. BERLEE (a cura di), *Research Handbook in Data Science and Law*, Cheltenham-Nothampton, Edward Elgar Publishing, 2018, pp. 378-407

DANIELE L., *Diritto dell'Unione europea*, Milano, Giuffrè, 2018

DANIELE L., *Diritto dell'Unione europea*, Torino, Giappichelli, 2014

DE BÚRCA G., *After the EU Charter of Fundamental Rights: the Court of Justice as a human rights adjudicator*, in *Maastricht Journal of European and Comparative Law*, n. 2/2013, pp. 168-184

DE CUPIS A., *I diritti della personalità*, Milano, Giuffrè, 1973

DE CUPIS A., *Teoria generale, diritto alla vita e all'integrità fisica, diritto sulle parti staccate del corso e sul cadavere, diritto alla libertà, diritto all'onore e alla riservatezza*, Milano, Giuffrè, 1958

DE HERT P., GUTWIRTH S., *Data Protection in the Case Law od Strasbourg and Luxemburg: Constitutionalisation in Action*, in S. GUTWIRTH ET AL (a cura di), *Reinventing Data Protection?*, Dordrecht, Springer, 2009

DE MARTIN J.C., *Introduzione,* a L. FLORIDI, *La rivoluzione dell'informazione* (titolo originale: *Information – A very short introduction*), Torino, Codice Edizioni, 2012.

DE MINICO G., *Costituzione. Emergenza e terrorismo*, Napoli, Jovene, 2016

DE MINICO G., *Le libertà fondamentali in tempo di ordinario terrorismo*, in *Federalismi.it*, 20 maggio 2015, n. 10/2015, pp. 2-28

DE TULLIO F.M., *La privacy e i big data verso una dimensione costituzionale collettiva*, in *Politica del diritto,* 4, 2016, pp. 637-696

DE VERGOTTINI G., *Guerra e Costituzione. Nuovi conflitti e sfide alla democrazia*, Bologna, Il Mulino, 2004

DE VRIES K., R. BELLANOVA, P. DE HERT, S. GUTWIRTH, *The German Constitutional Court judgement on data retention: Proportionality Overriddes unlimited surveillance (Doesn't it?)*, in S. GUTWIRTH, Y. POULLET, P. DE HERT, R. LEENES (a cura di), *Computers, Privacy and Data Protection: an Element of Choice*, Dordrecht, Springer, 2011

DEMEZTOU K., *GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved*, 2019

DI MARTINO A., *I profili costituzionali della privacy negli Stati Uniti e in Europa*, Jovene, Napoli, 2017

DI RESTA F., *La nuova privacy europea: i principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, Torino, Giappichelli, 2018

DICOSOLA M., *La* data retention directive *e il dialogo tra Corti costituzionali e Corte di Giustizia nel sistema multilivello europeo*, in *DirittiComparati.it*, 20 febbraio 2014

DONATI F., *Articolo 8 – La protezione dei dati di carattere personale*, in R. BIFULCO, M. CARTABIA, A. CELOTTO (a cura di), *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione europea*, Bologna, Il Mulino, 2001

DURICA J., *Directive on the Retention of Data on Electronic Communication in the Rulings of the Constitutional Courts of the EU Member States and Efforts for its Renewed Implementation*, in *The Lawyer Quarterly*, 2013, pp. 143-158

ESPOSITO C., *La libertà di manifestazione del pensiero nell'ordinamento italiano*, in *Rivista italiana di scienze giuridiche*, pp. 1957-1968

FALCONE M., *"Big data" e pubbliche amministrazioni. Nuove prospettive per la funzione conoscitiva pubblica*, in *Rivista trimestrale di diritto pubblico,* 3, 2017, pp. 601-639

FAMIGLIETTI G., *Il diritto alla riservatezza o la riservatezza come diritto. Appunti in tema di riservatezza ed* intimidad *sulla scorta della giurisprudenza della Corte costituzionale e del* Tribunal Constitucional, in A. D'ALOIA (a cura di), *Biotecnologie e valori costituzionali. Il contributo della giurisprudenza costituzionale*, Torino, Giappichelli, 2005

FEILER, L., *The Legality of the Data Retention Directive in Light of the fundamental Rights to Privacy and Data Protection*, in *European Journal of Law and Technology*, 2010

FENNELLY D., *Data retention: the life, death and afterlife of a directive,* in *ERA Forum*, Springer, 25 giugno 2018

FERRARI G.F., *I diritti fondamentali dopo la Carta di Nizza. Il costituzionalismo dei diritti*, Milano, Giuffrè, 2001

FERRARI G.F., *I diritti tra costituzionalismi statali e discipline transnazionali*, in ID. (a cura di) *I diritti fondamentali dopo la Carta di Nizza. Il costituzionalismo dei diritti*, Milano, Giuffrè, 2001

FERRARO F., LAZZERINI N., *Articolo 52 – Portata dei diritti garantiti*, in R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di) *La Carta dei Diritti Fondamentali dell'Unione Europea,* Milano, Giuffrè, 2017

FIGONE A., *Il diritto alla riservatezza dell'ordinamento francese, )*, in M. BESSONE, G. GIACOBBE (a cura di), *Il diritto alla riservatezza in Italia e ed in Francia,* Padova, Cedam, 1988

FINOCCHIARO G., *Introduzione,* in EAD. (diretto da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017

FINOCCHIARO G., *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, Roma, Roma Tre-Press, 2015

FLAHERTY D.H., *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*, Chapel Hill, University of North Carolina Press, 1989

FLORIDI L. *Hyperhistory and the Philosophy of Information Policies*, in L. FLORIDI (a cura di) *The Onlife Manifesto*, Springer, 2013

FLORIDI L., *La rivoluzione dell'informazione,* Torino, Codice Editore, 2012

FLORIDI L., *Quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, Cortina Editore, 2017

FOA S., *Il trattamento dei dati personali per finalità di rilevante interesse pubblico*, in G. SANTANIELLO (diretto da), *Trattato di diritto amministrativo*, Vol. XXXVI, *La protezione dei dati personali*, Padova, Cedam, 2005

FOIS S., *Principi costituzionali e libertà di manifestazione del pensiero*, Milano, Giuffrè, 1957

FONTANELLI F., *La Corte di Giustizia e il "favor communitatis". Il percorso della giurisprudenza della Corte di Giustizia delle Comunità europee sul fondamento normativo degli atti dell'Unione*, in *Rivista italiana di diritto pubblico comunitario*, 2010, pp. 177-202

FORGÓ N., S. HÄNOLD, B. SCHÜTZE, *The Principle of Purpose Limitation and Big Data*, in M. CORRALES, M. FENWICK, N. FORGÓ (a cura di), *New Technology, Big Data and the Law*, Singapore, Springer, 2017, pp. 17-42

FORMICI G., *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia* Ministerio Fiscal*,* in *Osservatorio Costituzionale*, n. 3/2018, pp. 453-467

FRIEDMAN B., H. NISSENBAUM, *Bias in Computer Systems*, in *ACM Transactions on Information Systems (TOIS)* 14/1996, pp. 330-347

FRONTONI E., *La giurisprudenza costituzionale*, in A. CLEMENTE (a cura di), *Privacy*, Padova, Cedam, 1999

FROSINI A., *Gli atti normativi del Garante per la protezione dei dati personali*, in *Giurisprudenza costituzionale*, 2014, pp. 3679-3708

FROSINI T.E., *Liberté, Egalité, Internet*, Napoli, Editoriale Scientifica, 2015

FROSINI V., *1984. L'informatica nella società contemporanea* (I), *Informatica e diritto*, 1984, pp. 7-15

FROSINI V., *1984. L'informatica nella società contemporanea* (II), *Informatica e diritto*, 2001, pp. 133-144

FROSINI V., *Banche dati e tutela della persona*, in *Informatica diritto e società*, 1988

FROSINI V., *La Convenzione Europea sulla protezione dei dati*, in *Rivista di Diritto Europeo* 24, 1984, pp. 3-18

FROSINI V., *La protezione della riservatezza nella società informatica*, in *Informatica e diritto*, 2001, pp. 85-96

GAMBARO G., PARDOLESI R., *L'influenza dei valori costituzionali sul diritto civile*, in A. PIZZORUSSO, V. VARANO (a cura di), *L'influenza dei valori costituzionali sui sistemi giuridici contemporanei*, Milano, Giuffrè, 1985

GELLERT R., *Data Protection: a risk regulation? Between the risk management of everything and the precautionary alternative*, in *International Data privacy Law*, 5, 2015, pp. 3-19

GELLERT R., *Understanding the notion of risk in the General Data Protection Regulation*, in *Computer Law and Security Review*, 2017, pp. 279-288

GENNUSA M.E., I. CANOR, *Il caso Kadi in tema di sicurezza*, in M. CARTABIA (a cura di), *Dieci casi sui diritti in Europa*, Bologna, Il Mulino, 2011

GENNUSA M.E., *La Cedu e l'Unione europea*, in M. CARTABIA (a cura di), *I diritti in azione*, Bologna, Il Mulino, 2007

GIAMPICCOLO G., *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, in *Rivista trimestrale di diritto e procedura civile*, 1958

GIANNITI P., *La «comunitarizzazione» della «Carta» a seguito del Trattato di Lisbona*, in ID. (a cura di), *I diritti fondamentali nell'Unione Europea*, *La Carta di Nizza dopo il Trattato di Lisbona*, Bologna, Zanichelli, 2013

GLENDON M.A., *I diritti nelle Costituzioni del ventesimo secolo*, in ID. (a cura di), *Tradizioni in subbuglio* (trad. it. a cura di P.G. Carozza e M. Cartabia), Soveria Mannelli, Rubettino, 2007

GONZÁLEZ FUSTER G., GELLERT R., *The fundamental right of data protection in the European Unione: in serach of an uncharted right*, in *International Review of Law, Computers & Technology*, 26(1), 2012, pp. 73-82

GONZÁLEZ FUSTER G., H. HIJMANS, *The EU rights to privacy and personal data protection: 20 years in 10 questions***,** discussion paper, 14 maggio 2019

GONZÁLEZ FUSTER G., *The emergence of data protection as a fundamental right of EU*, Heidelberg, Springer, 2014

GRANARA D., *Ricostruire il diritto all'identità personale: il diritto all'oblio e la libertà di informazione*, in *Diritto pubblico comparato*, n. 3/2014, pp. 1253-1259

GREMENTIERI P., *Il processo comunitario. Principi e garanzie fondamentali*, Milano, Giuffrè, 1973

GRISOLIA A., *Alcune considerazioni sul potere normativo del Garante per la protezione dei dati personali dalla l. n. 675/1996 al "Codice in materia di protezione dei dati personali",* in P. CARETTI (a cura di), *Osservatorio sulle fonti, 2003/2004. I poteri normativi delle autorità indipendenti*, Torino, Giappichelli, 2005

GROPPI T., *Art. 52 Portata dei diritti garantiti*, in R. BIFULCO, M. CARTABIA, A. CELOTTO (a cura di), *L'Europa dei diritti*, Bologna, Il Mulino, 2001

GROPPI T., *Articolo 7*, in R. BIFULCO, M. CARTABIA, A. CELOTTO (a cura di), *L'Europa dei diritti*, Bologna, Il Mulino, 2001

GROSSO E., *Autorità indipendente o autorità onnipotente? Il potere normativo di fatto del garante per la protezione dei dati personali,* in M. LOSANO (a cura di), *La legge italiana sulla* privacy, Roma, Laterza, 2001

GUARDIGLI E., *Le Autorità di controllo*, in G. FINOCCHIARO (diretto da), *Il nuovo regolamento europeo sulla privacy*, Bologna, Zanichelli, 2017

GUARINI C.P., *«Maschio e femmina li creò…» o, forse, no. La Corte costituzionale ancora sulla non necessità di intervento chirurgico per la rettificazione anagrafica di attribuzione di sesso*, in *Federalismi*, 8/2018

GUELLA F., Data retention *e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali*, in *Diritto pubblico comparato ed europeo – online*, 2/2017, pp. 349-357.

GUTWIRTH S., *Privacy and the Information Age*, New York-Oxford, Lanham & Boulder 2002

HARRIS S.J., J.M. WYNDHAM, *Data Rights and Responsibilities: A Human Rights Perspective on Data Sharing*, in *Journal of Empirical Research on Human Research Ethics*, n.10/2015, pp. 334-337

HEIL H., *Directive 95/46/EC of the European Parliament and of the Council: Introductory Remarks,* in A. BÜLLESBACH et al. (a cura di), *Concise European IT Law*, Alphen aan den Rijn, Kluwer International Law, 2010

HIJMANS H., *The European Uninon as Guardian of Internet Privacy. The Story of the Article 16 TFEU*, Dordrecht , Springer, 2016

HIJMANS H., *The European Union as a constitutional guardian of internet privacy and data protection*, tesi di dottorato, 2016

HILDELBARNDT M., L. TIELEMANS, *Data protection by design and technology neutral law*, in *Computer Law & Security Review*, 29/2013, pp. 509-521

HOLMES D.E., *Big Data. A very short introduction*, Cambridge, Cambridge University Press, 2014

HONDIUS F.W., *Emerging Data Protection in Europe*, Amsterdam, North-Holland Publishing Company, 1975

IADICICCO M.P., *La diagnosi genetica preimpianto nella giurisprudenza italiana ed europea. L'insufficienza del dialogo tra le Corti*, in *Quaderni costituzionali*, 2/2015, pp. 325-350

JNAZU J., *Virtual Assembly*, in *Cornell Law Review*, 2013, pp. 1093-1142, spec. pp. 1118 ss.

KAMINSKI M.E., *The Right to Explanation, Explained*, in *Berkeley Technology Law Review*, 134/2019, pp. 189-218

KLONICK K., *The New Governors: The People, Rules and Process Governing Online Speech*, in *Harvard La Review*, 2018, pp. 1599-1670

KOSTA E., *The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Protection Directive with the Rights to Privacy and Data Protection*, in *Scripted*, 2013

KROLL A.J., HUEY J., BAROCAS S., FELTEN E.W., REIDENBERG J.R., ROBINSON D.G., YU H., *Accountable Algorithms*, in *University of Pennsylvania Law Review,* 165/2017, pp. 633-705

KULK G., ZUIDERVEEN F., BORGESIUS N., *Privacy, freedom of expression, and the right to be forgotten in Europe*, in O. TENE, J. POLONETSKY, E. SELINGER (a cura di), *Cambridge Handbook of Consumer Privacy*, Cambridge, Cambridge University Press, 2017

LANEY D., *3D Management: Controlling Data Volume, Velocity and Variety,* MetaGroup (Gartner Data & Analytics), File 949, 6 febbraio 2001).

LAUDON K.C., *Dossier Society: Value Choices in the Design of National Information Systems*, New York, Columbia University Press, 1986

LONGO E., *I trattamenti nel settore dell'istruzione e a fini di ricerca (scientifica, storica, statistica,* in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, Napoli, Editoriale Scientifica, 2017

LOSANO M., *Il diritto pubblico nell'informatica,* Torino, Einaudi, 1986

LUCIANI M., *Diritti sociali e integrazione europea*, in *Politica del diritto*, 2000, pp. 367-405

LUCIANI M., *Il brusco risveglio. I controlimiti e la fine mancata della storia costituzionale*, in A. BERNARDI (a cura di), *I controlimiti. Primato delle norme europee e difesa dei principi costituzionali*, Napoli, Jovene, 2017

LYNSKEY O., *The Foundation of EU Data Protection Law*, Oxford, Oxford University Press, 2015

MACARIO F., *La protezione dei dati personali nel diritto privato italiano*, in V. CUFFARO, V. RICCIUTO (a cura di), *La disciplina del trattamento dei dati personali*, Torino, Giappichelli, 1997

MALGIERI G., *Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations*, in *Computer Law and Security Review*, 2019 (disponibile *online*).

MALGIERI G., G. COMANDÉ, *Why a Right to Legibility of Automated Decisione-Making Exists in the General Data Protection Regulation*, in *International data Privacy Law*, 7(4), 2017, pp. 243-265.

MANTELERO A., *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era*, in B. VAN DER SLOOT, L. FLORIDI, L. TAYLOR (a cura di), *Group Privacy*, Verlag, Springer, 2017, pp. 139-158

MANTELERO A., *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva*, in G. FINOCCHIARO (diretto da), *Il nuovo regolamento europeo sulla privacy*, Bologna, Zanichelli, 2017

MANTELERO A., *La privacy all'epoca dei big data*, in V. CUFFARO, R. D'ORAZIONE, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit.,

MANTELERO A., *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection*, in *Computer Law & Security Review*, 32/2016, pp. 238-255 (spec. pp. 241 e 145)

MANZELLA A., *Dal mercato ai diritti*, in A. MANZELLA, P. MELOGRANI, E. PACIOTTI, S. RODOTÀ (a cura di), *Riscrivere i diritti in Europa*, Bologna, Il Mulino, 2001

MARR B., *Here's Why Data Is Not The New Oil*, in *Forbes*, 5 maggio 2018

MASERA A., SCORZA G., *Internet, i nostri diritti*, Roma, Laterza, 2016

MASSA PINTO I., *Il bilanciamento degli interessi nella legge sulla privacy*, in M. LOSANO (a cura di), *La legge italiana sulla* privacy, Roma, Laterza, 2001

MASTROIANNI R., *Art. 47 TUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea e della Comunità europea*, Milano, 2004

MAYER-SCHÖNBERGER V., CUCKIER K., *Learning with Big Data: The Future of education,* Boston, Houghton Mifflin Harcourt, 2014

MAYER-SCHÖNBERGER V., CUKIER K., *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, Garzanti, 2013

MAYER-SCHÖNBERGER V., *Generational Development of Data Protection in Europe*, in P.E. AGRE, M. ROTENBERG (a cura di), *Technology and Privacy: The New Landscape*, Cambridge(MA)-Londra, MIT Press, 1997

MAZZIOTTI DI CELSO M., *Diritto all'immagine e Costituzione* in *Diritto e società,* 4/1979, pp. 911-920

MICKLITZ H.W., *Introduzione*, in ID. (a cura di) *Constitutionalization of European Private Law*, Oxford, Oxford University Press, 2014

MILAZZO P., *La Direttiva UE 2016/680 e la protezione dei dati personali nell'ambito della sicurezza pubblica e della giustizia penale*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/ 679*, Napoli, Editoriale Scientifica, 2017

MIRABELLI C., *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *Diritto dell'informatica e dell'informazione*, 1993, pp. 313-330

MODUGNO F., *I "nuovi" diritti nella giurisprudenza costituzionale*, Torino, Giappichelli, 1995

MORELLI A., *I diritti senza legge*, in *Consulta online*, 2015

MORELLI S., *Tecniche di tutela dei diritti fondamentali della persona: nuovi diritti nella giurisprudenza della Corte costituzionale, di Cassazione, europea di Strasburgo, tutela preventiva e risarcitoria*, Padova, Cedam, 2003

MUÑOZ C., *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights,* White House, Executive Office of the President, maggio 2016

MUÑOZ C., SMITH M., PATIL D., *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, The White House, Executive Office of the President, maggio 2016

MURPHY C., *Romanian Constitutional Court, Decision No. 1258 of 8 October 2009*, in *Common Market Law Review*, 47/2010, pp. 933-941

NIGER S., *Le nuove dimensione della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, Cedam, 2006

OREFICE M., *Gli open data tra principio e azione: lo stato di avanzamento*, in *Forum di Quaderni Costituzionali,* 2015

OROFINO M., *La libertà di espressione tra Costituzione e Carte europee dei diritti*, Torino, Giappichelli, 2014

OROFINO M., *Trattamento dei dati personali e libertà di espressione e informazione*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, Napoli, Editoriale Scientifica, 2017

PACE A., *A che serve la Carta dei diritti fondamentali dell'Unione Europea? Appunti preliminari*, in *Giurisprudenza costituzionale*, 1/2001, pp. 193-207

PACE A., *Problematiche delle libertà costituzionali. Parte generale*, 3° ed. agg., Padova, Cedam, 2003

PACILEO P., *Il diritto alla portabilità*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea sulla privacy*, Padova, Cedam, 2016

PACIOTTI E., *La Carta: i contenuti, gli autori*, in A. MANZELLA, P. MELOGRANI, E. PACIOTTI, S. RODOTÀ (a cura di), *Riscrivere i diritti in Europa*, Bologna, Il Mulino, 2001

PACKARD V., *The Naked Society*, Harmondsworth, Penguin Books, 1971

PAGANO R., *Aspetti economici e giuridici delle banche dati*, in *Informativa e diritto*, 1986, pp. 975-977

PAGANO R., *Tutela dei dati personali: evoluzione della legislazione europea e stato del dibattito*, in *Informatica e diritto*, 1986, pp. 67-94

PALADINI L., *I conflitti fra pilastri dell'Unione europea e le prospettive del Trattato di Lisbona*, in *Il Diritto dell'Unione europea*, 2010, pp. 87-107

PALLARO P., *Libertà della persona e trattamento dei dati personali nell'Unione europea*, Milano, Giuffrè, 2002

PALMIERI A., *Trattamento dei dati personali e giornalismo: alla ricerca di un equilibrio stabile*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, II, Milano, Giuffrè, 2003

PANETTA R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato: commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice privacy): scritti in memoria di Stefano Rodotà*, Milano, Giuffrè, 2019

PARDOLESI R., *L'ombra del tempo e (il diritto al) l'oblio*, in *Questione giustizia*, n. 1/2017, pp. 76-86

PARISER E., *Il filtro. Quello che internet ci nasconde*, Milano, Il Saggiatore, 2012

PASQUALE F., *The Black Box Society*, *The Secret Algorithms That Control Money and Information*, Cambridge, 2016

PASSAGLIA P., *Corte costituzionale e diritto dell'Internet: un rapporto difficile (e un appuntamento da non mancare)*, in *Giurisprudenza Costituzionale,* 6/2014, pp. 4837-4865

PASSAGLIA P., *Il sistema delle fonti normative in materia di tutela dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo, Torino*, Giappichelli, 2019

PATRONI GRIFFI A., *L'indipendenza del Garante*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE2016/679*, Napoli, Editoriale Scientifica, 2017

PETKOVA B., *Domesticating the 'Foreign' in Making Data Privacy Law*, in *International Journal of Constitutional Law,* 15(4)/2017, pp. 1135–1156

PETKOVA B., *Towards an Internal Hierarchy of Values in the EU Legal Order: Balancing the Freedom of Speech and Data Privacy*, in *Maastricht Journal of European and Comparative Law* 23 (3), 2016, pp. 421-438

PICIOCCHI C., *I diritti inviolabili*, in C. CASONATO (a cura di), *Lezioni sui principi fondamentali della Costituzione*, Torino, Giappichelli, 2008

PINELLI C., *Il preambolo, i valori, gli obiettivi*, in BASSINI F., TIBERI G. (a cura di), *Una Costituzione per l'Europa. Dalla Convenzione europea alla Conferenza intergovernativa*, Bologna, Il Mulino, 2003

PINO G., *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, Il Mulino, 2003

PIZZETTI F. (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018

PIZZETTI F. (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, Giappichelli, 2018

PIZZETTI F., *Le competenze dell'Unione*, in BASSINI F., TIBERI G. (a cura di), *Una Costituzione per l'Europa. Dalla Convenzione europea alla Conferenza intergovernativa*, Bologna, Il Mulino, 2003

PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali*, vol. II, *Il Regolamento europeo 2016/679*, Torino, Giappichelli, 2016

PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali*, vol. I, *Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, Giappichelli, 2016

PIZZETTI F., *Sette anni di protezione dei dati in Italia,* Torino, Giappichelli, 2012

PIZZORUSSO A., *Il patrimonio costituzionale europeo*, Bologna, Il Mulino, 2002

PODESTA J. et al., *Big Data: Seizing Opportunities, Preserving Values,* White House, Executive Office of the President, maggio 2014

POGGI A., *Dati personali. Una soluzione "giurisdizionale" oppure "amministrativa" per l'effettiva tutela del cittadino?*, in M. LOSANO (a cura di), *La legge italiana sulla privacy*, Roma, Laterza, 2001

POLLICINO O., BASSINI M., *Articolo 8 – La protezione dei dati di carattere personale*, in R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di) *La Carta dei Diritti Fondamentali dell'Unione Europea,* Milano, Giuffrè, 2017

POLLICINO O., G.E. VIGEVANI, *Privacy digitale e conservazione dei dati di traffico per finalità di sicurezza: la sentenza* Tele2 Sverige *della Corte di giustizia UE*, in *Forum di Quaderni costituzionali*, 16 gennaio 2017

POLLICINO O., M. BASSINI, *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Diritto Penale Contemporaneo*, 2017, pp. 1-10

POLLICINO O., *Not to be Pushed Aside: the Italian Constitutional Court and the European Court of Justice*, in *Verfassungsblog – on matters constitutional*, 27 febbraio 2019

POLLICINO O., *Un* digital rights to privacy *preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel* reasoning *di Google Spain*, in *Diritto dell'informazione e dell'informatica*, 2014, pp. 569-589

POTESTA J., *Big Data: Seizing Opportunities, Preserving Values* ("Rapporto Potesta"), Ufficio esecutivo del presidente, Washington, maggio 2014

PURTOVA N., *The law of everything. Broad concept of personal data and future of EU data protection law*, in *Law, Innovation and Technology*, 2018, pp. 40-81

QUELLE C., *The Data Protection Impact Assessment, or: How the General Data Protection Regulation May Still Come to Foster Ethically Responsible Data Processing*, research paper, 25 novembre, 2015

RAAB C., D. WRIGHT, *Surveillance: Extending the Limits of Privacy Impact Assessment*, in D. WRIGHT, P. DE HERT (a cura di), *Privacy Impact Assessment*, Dordrecht, Springer, 2012

REALE C.M., *Corte costituzionale e trasgendersimo: l'irriducibile varietà delle singole situazioni*, in *Rivista di Biodiritto*, 1, 2016, pp. 283-295

RESTA G., *Identità personale e identità digitale*, in *Il diritto dell'informazione e dell'informatica*, 2007, pp. 511-531

RESTA G., *Il diritto alla protezione dei dati personali*, in F. CARDARELLI, S. SICA, V. ZENO ZENCOVICH (a cura di), *Il codice dei dati personali: temi e problemi*, Milano, Giuffrè, 2004

REZZANI A., *Big Data: Architettura, tecnologie e metodi per l'utilizzo di grandi basi di dati*, Milano, Apogeo, 2014

RODOTÀ S., *Data Protection as a Fundamental Right*, in S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE, S. NOUWT (a cura di), *Reinventing Data Protection?,* New York, Springer, 2009

RODOTÀ S., *Elaboratori elettronici e controllo sociale*, Bologna, Il Mulino, 1974

RODOTÀ S., *Il mondo nella rete. Quali diritti, quali vincoli*, Roma, Laterza, 2014

RODOTÀ S., *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma, 2014

RODOTÀ S., *La privacy tra individuo e collettività,* in *Politica del diritto,* 1974

RODOTÀ S., Privacy *e costruzione della sfera privata. Ipotesi e prospettive*, in *Politica del diritto*, 1991

RODOTÀ S., *Repertorio di fine secolo,* Roma, Laterza, 1999

RODOTÀ S., *Tecnopolitica. La democrazia e le nuove forme di comunicazione*, Laterza, Roma-Bari, 2004

ROMANO C., Open data *e riutilizzo nel decreto trasparenza: propulsore per la democrazia e lo sviluppo o sfida ulteriore per i diritti fondamentali?*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Napoli, Editoriale Scientifica, 2014

ROMBOLI R., *Dalla «diffusione» all'«accentramento»: una significativa linea di tendenza della più recente giurisprudenza costituzionale*, in *Foro Italiano*, n. 143/2018, pp. 2226-2236

ROUVROY A., PULLET Y., *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy?*, in S.

GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE, S. NOUWT (a cura di), *Reinventing Data Protection?,* New York, Springer, 2009

RUBECHI M., *La transizione verso il nuovo sistema delle fonti europee di protezione dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2017

RUGGERI A., *La Consulta rimette a punto di i rapporti tra diritto eurounitario e diritto interno con una pronunzia in chiaro scuro (A prima lettura i Corte cost. nt. n. 20 del 2019)*, in *Consulta Online*, 25 febbraio 2019

RUGGERI A., *Primato del diritto sovranazionale versus identità costituzionale? (Alla ricerca dell'araba fenice costituzionale: i «controlimiti»)*, in, A. BERNARDI (a cura di), *I controlimiti. Primato delle norme europee e difesa dei principi costituzionali*, Napoli, Jovene, 2017

RUGGERI A., *Svolta della Consulta sulle questioni di diritto eurounitario assiologicamente pregnanti, attratte nell'orbita del sindacato accentrato di costituzionalità, pur se riguardanti norme dell'Unione self-executing (a margine di Corte cost. n. 269 del 2017)*, in *Rivista di Diritti Comparati*, n. 3/2017, pp. 234-247

SALERNO G.M., *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in R. NANIA, P. RIDOLA (a cura di), *I diritti costituzionali*, Torino, Giappichelli, 2006

SALMONI F., *Controlimiti, diritti con lo stesso* nomen *e ruolo accentrato della Consulta. L'integrazione del parametro con le fonti europee di diritto derivato e il sindacato sulla "conformità" alla Costituzione e la mera "compatibilità" con la Carta dei diritti fondamentali dell'UE*, in *Federalismi.it,* 17 aprile 2019, n. 8/2019, pp. 1-20

SARTOR G., *The right to be forgotten: Balancing interests in the flux of time*, in *International Journal of Law and Information Technology*, 24/2016, pp. 72-98

SCACCIA G., *Giudici comuni e diritto dell'Unione europea nella sentenza della Corte costituzionale n. 269 del 2017*, in *Giurisprudenza costituzionale*., n. 6/2017, pp. 1-8

SCACCIA G., *L'inversione della "doppia pregiudizialità" nella sentenza della Corte costituzionale n. 269 del 2017: presupposti teorici e problemi applicativi*, in *Forum di Quaderni Costituzionali*, 25 gennaio 2018

SCHULHOFER S.J., *An International Right to Privacy? Be Careful What You Wish for*, in *International Journal of Constitutional Law*, 2016, pp. 238-261

SCORZA G., *Prospettive* de iure condendo *della protezione dei dati personali nel settore delle comunicazioni elettroniche, tra Regolamento generale 2016/679 e futuro Regolamento e-Privacy*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2017

SELBST A.D., POWLES J., *Meaningful information and the right to explanation*, in *International Data Privacy Law*, 4/2017, pp. 233-242

SESSO SARTI O., *Profilazione e trattamento dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologia e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, cit.

SHADMY T., *The New Social Contract: Facebook's Community and Our Rights*, in *Boston International Law Review* 2019 (in corso di pubblicazione)

SHROFF G., *The Intelligent Web. Search, Smart Algorithms, and Big data,* Oxford, Oxford University Press, 2015

SICA S., STANZIONE P. (a cura di), *La nuova disciplina della privacy. Commento al d.lgs. 30 giugno 2003, n. 196*, Bologna, Zanichelli, 2005

SIMONCINI A., *Autorità indipendenti e 'costruzione dell'ordinamento giuridico': il caso del Garante per la protezione dei dati personali*, in *Diritto Pubblico*, 2009, pp. 851-989

SIMONCINI A., *I codici deontologici di protezione dei dati personali nel sistema delle fonti. L'emersione di un nuovo paradigma normativo*, in U. DE SIERVO (a cura di), Osservatorio sulle fonti 1999, Torino, Giappichelli, 2000

SIMONCINI A., *Il sistema delle fonti normative*, in V. CUFFARO, V. RICCIUTO (a cura di), *Il trattamento dei dati personali*, vol. II, *Profili applicativi*, Torino, Giappichelli, 1999,

SIMONCINI A., *L'algoritmo incostituzionale: intelligenza artificiale e futuro delle libertà*, in *Rivista Biodiritto – BioLaw Journal*, n. 1/2019, pp. 63-89

SIMONCINI A., S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 1/2019, pp. 87-106

SIMONCINI A., *Sovranità e potere nell'era digitale*, in O. POLLICINO, T.E. FROSINI, E. APA, M. BASSINI (a cura di), *Diritti e libertà in Internet*, Milano, Mondadori, 2017

SORO A., *La società sorvegliata. I nuovi confini della libertà*, in Garante per la protezione dei dati personali (a cura di), *Atti del Convegno del 28 gennaio 2016*

SPANGARO A., *L'ambito di riferimento materiale del nuovo Regolamento*, in G. FINOCCHIARO (diretto da) *Il nuovo Regolamento europeo sulla privacy*, Bologna, Zanichelli, 2017

SPINA A., *Risk Regulation of Big Data: Has the Time Arrived for a Paradigm Shift in EU Data Protection Law?*, in *European Journal of Risk Regulation*, n. 2/2014, pp. 248-252

SUSTEIN C.R., *Il costo dei diritti*, Bologna, Il Mulino, 2000

*The world's most valuable resource is no longer oil, but data. The data economy demands a new approach to antitrust rules*, in *The Economist*, 6 maggio 2017

TIBERI G., *Il caso* Tele2 Sverige/Watson: *un'*iconica *sentenza della Corte di Giustizia nella saga sulla* data retention*,* in *Quaderni costituzionali*, 2017, pp. 434-438

TIBERI G., *Riservatezza e protezione dei dati personali*, in M. CARTABIA (a cura di), i *Diritti in azione*, Bologna, Il mulino, 2007

TIEGHI G., *Per una «Costituzione continuamente attualizzata»: Corte costituzionale e* overruling, in M. BERTOLISSI (a cura di), *Riforme. Opinioni a confronto*, Napoli, Jovene, 2015

TISNE M., *It's time for a Bill of Data Rights,* in *MIT Technology Review*, 14 dicembre 2018

TORINO R., *La valutazione di impatto (Data Protection Impact Assessment)*, in V. CUFFARO, R. D'ORAZIONE, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019

TORRES C., A. SHAHSHAHANI, T. TAVARAS, *Indiscriminate Power: Racial Profiling and Surveillance since 9/11*, in *University of Pennsylvania Journal of Law and Social Change* 2015-16, pp. 283-310

TOSCHEI S., *I trattamenti in ambito pubblico nell'era della digitalizzazione e della trasparenza*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2017

TOURI K., *The Many Constitutions of Europe*, in K. TOURI, S. SANKARI (a cura di), *The Many Constitutions of Europe*, New York, Routlege, 2016

TRUCCO L., *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale*, Torino, Giappichelli, 2004

TZANOU M., *The Fundamental Right to Data Protection. Normative Value in the Context of Counter-Terrorism Surveillance*, Oxford-Portland (Oregon), Hart Publiching, 2017

VAN ALSENOY B., *Data Protection Law in the EU: Roles, Responsibility and Liability*, Anversa, Intersentia, 2019

VAN DIJK N., GELLERT R., ROMMETVEIT K., *A Risk to a Right? Beyond Data Protection Impact Assessment*, in *Computer Law and Security Review*, 32, 2016, pp. 286-306

VANNI D., *La protezione dei dati personali in prospettiva comparatistica*, Roma, Aracne, 2012

VEDASCHI A., *À la guerre comme à a la guerre? La disciplina della guerra nel diritto costituzionale comparato*, Torino, Giappichelli, 2007

VEDASCHI A., *I programmi di sorveglianza di massa nello Stato di diritto. La "data retention" al test di legittimità*, in *Diritto pubblico comparato ed europeo*, 2014, pp. 1224-1245

VEDASCHI A., LUBELLO V., *Data Retention and its Implications for the Fundamental Right to Privacy*, *Tilburg Law Review*, 2015, pp. 14-34

VERNUCCIO S., *La sentenza 269/2017: la Corte costituzionale di fronte alla questione dell'efficacia diretta della Carta di Nizza e la prima risposta del giudice comune (Cass. ord. 3831/2018)*, in *Osservatorio Costituzionale*, n. 2/2018. pp. 1-20

VIGATO E., *Godelli c. Italia. Il diritto a conoscere le proprie origini*, in *Quaderni costituzionali*, 4, 2012, pp. 908-910

VIGGIANO M., *I limiti alla pubblicità dell'azione amministrativa per finalità d trasparenza derivanti dalla protezione dei dati personali,* , in L. CALIFANO, C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Napoli, Editoriale Scientifica, 2014

WACHTER S., B. MITTELSTADT, C. RUSSELL, *Counterfactual explanations without opening the Black Box: automated decisions and the GDPR,* in *Harvard Journal of Law & Technology*, 31(2)/2018, pp. 842-887

WACHTER S., MITTELSTADT B., FLORIDI L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2/2017, pp. 76-99

WARNIER M., F. DECHESNE, F. BRAZIER, *Design for the Value of Privacy*, in J. VAN DEN HOVEN. P.E. VERMAAS, I. VAN DE POEL (a cura di), *Handbook of Ethics, Values, and Technological Design. Sources, Theory, Values and Application Domains*, Dorcrecht, Springer, 2015

WEILER J.H.H., *Eurocracy and Distrusts. Some Questions Concerning the Role of the European Court of Justice in the Protection of Fundamental Human Rights withtin the Legal Order of the European Communities*, in *Washington Law Review*, 1986

WEILER J.H.H., *Il sistema comunitario europeo. Struttura giuridica e processo politico,* Bologna, Il Mulino, 1985

WEILER J.H.H., *La Costituzione dell'Europa*, Bologna, Il Mulino, 1999

WESTIN A.F., BAKER M.A., *Data banks in a Free Society*, New York, Quadrangle Books, 1972

WESTIN A.F., *Privacy and Freedom*, New York, Athenaeum, 1970

YEUNG K., *Algorithmic Regulation: A Critical Interrogation*, in *Regulation & Governance*, 31 luglio 2017

YEUNG K., *Desing for the Value of Regulation*, *ibidem*, in J. VAN DEN HOVEN. P.E. VERMAAS, I. VAN DE POEL (a cura di), *Handbook of Ethics, Values, and Technological Design. Sources, Theory, Values and Application Domains*, Dorcrecht, Springer, 2015

YEUNG K., *Towards an understanding of regulation by design*, in R. BROWNSWORD, K. YEUNG (a cura di) *Regulating technology*, Oxford, Hart Publishing, 2008

ZAGREBELSKY G., *Costi europee e corti nazionali*, Resoconto della Relazione al Seminario dell'Osservatorio costituzionale della LUISS su *I mutamenti costituzionali in Italia nel quadro dell'integrazione europea*, 12 gennaio 2002

ZAGREBELSKY G., *Il diritto mite*, Torino, Einaudi, 1992

ZEMBRANO V., *Il Comitato europeo per la protezione dei dati*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019

ZENO ZENCOVICH V., *Telematica e diritto all'identità personale,* in *Politica del Diritto*, 1983

ZILLER J., *Articolo 51 – Ambito di applicazione*, in R. MASTROIANNI, A. ALLEGREZZA, O. RAZZOLINI, O. POLLICINO (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, Giuffrè, 2017

Giurisprudenza

*Corte costituzionale italiana*


Corte cost., ord. n. 369 del 2006
Corte cost., ord. n. 37 del 1995
Corte cost., sent. 235 del 1993
Corte cost., sent. 238 del 1996
Corte cost., sent. 257 del 1996
Corte cost., sent. n. 1 del 1981
Corte cost., sent. n. 1031 del 1988
Corte cost., sent. n. 105 del 1972
Corte cost., sent. n. 112 del 1993
Corte cost., sent. n. 115 del 2018
Corte cost., sent. n. 116 del 2006
Corte cost., sent. n. 12 del1972
Corte cost., sent. n. 120 del 2001
Corte cost., sent. n. 122 del 1970
Corte cost., sent. n. 13 del 1994
Corte cost., sent. n. 135 del 2002
Corte cost., sent. n. 138 del 1985
Corte cost., sent. n. 139 del 1990
Corte cost., sent. n. 150 del 2005
Corte cost., sent. n. 151 del 1986
Corte cost., sent. n. 151 del 2009
Corte cost., sent. n. 155 del 2002
Corte cost., sent. n. 162 del 2014
Corte cost., sent. n. 170 del 1984
Corte cost., sent. n. 173 del 2009
Corte cost., sent. n. 194 del 1987
Corte cost., sent. n. 20 del 2017
Corte cost., sent. n. 20 del 2019
Corte cost., sent. n. 210 del 1987
Corte cost., sent. n. 218 del 1994
Corte cost., sent. n. 225 del 1977
Corte cost., sent. n. 229 del 2015
Corte cost., sent. n. 27 del 1975
Corte cost., sent. n. 271 del 2005
Corte cost., sent. n. 272 del 2017
Corte cost., sent. n. 287 del 2013
Corte cost., sent. n. 327 del 2003
Corte cost., sent. n. 347 del 1998
Corte cost., sent. n. 366 del 1991
Corte cost., sent. n. 372 del 2006
Corte cost., sent. n. 373 del 1992
Corte cost., sent. n. 38 del 1973
Corte cost., sent. n. 617 del 1987
Corte cost., sent. n. 63 del 1994
Corte cost., sent. n. 63 del 2019
Corte cost., sent. n. 64 del 1998
Corte cost., sent. n. 641 del 1987
Corte cost., sent. n. 679 del 2017
Corte cost., sent. n. 81 del 1993
Corte cost., sent. n. 84 del 2016
Corte cost., sent. n. 96 del 2015
Corte cost., sent. n.122 del 1972


*Corte di cassazione italiana*


Cass, sent. 17 maggio 1975, n. 2129
Cass. sent. 9 novembre 2016, n. 22838
Cass., sent. 20 aprile 1963, n. 990
Cass., sent. 22 dicembre 1956, n. 4487
Cass., sent. 27 maggio 1975, n. 2129
Cass., sent. 20 marzo 2018, n. 6963
Cass., sent. 22 giugno 1985, n. 3769
Cass., sent. 7 febbraio 1996, n. 978

*Giurisprudenza straniera*


Corte costituzionale federale tedesca, del 15 dicembre 1983, *Volkszählungsurteil* (BVerfGE (65) 1983

Corte costituzionale federale tedesca, sent. 22 ottobre 1986*, Solange II* (BverfGe 73, 339)

Corte costituzionale federale tedesca, sent. 29 maggio 1974, *Solange I* (BVerfGE 37, 217)

Corte costituzionale federale tedesca, sent. 2 marzo 2010, *Vorratsdatenspeicherung* (1 BvR 256/08)

Corte costituzionale romena, sent. 8 ottobre 2009, n. 1258

Corte costituzionale romena, sent. 8 ottobre 2009, n. 1258, p. 9 del testo in lingua inglese

Corte suprema di Cipro, sent. 1 febbraio 2022 sui ricorsi nn. 65/2009, 78/2009, 82/2009, 15/2010, 22/2010

Tribunale amministrativo supremo della Bulgaria, sent. 11 dicembre 2008, n. 13627


*Corte di Giustizia delle Comunità europee (CGCE)*


CGCE, sent. 17 dicembre 1970, *Internationale Handelsgesellschaft* (causa C-11/70)

CGCE, sent. 1 aprile 1965, *Avv. Marcello Sgarlata et al. c. Commissione* (causa C-40/65)

CGCE, Sent. 10 febbraio 2009, *Irlanda/Parlamento e Consiglio* (causa C-301/06)

CGCE, sent. 12 novembre 1969, *Erich Stauder c. città di Ulm-Sozialamt* (causa C-29/69)

CGCE, sent. 14 maggio 1974, *J. Nold, Kohlen- und Baustoffgroßhandlung c. Commissione delle Comunità europee*, (causa C-4/73)

CGCE, sent. 15 luglio 1964, *Flaminio Costa c. Enel* (causa C-6/64)

CGCE, sent. 15 maggio 1986, *Marguerite Johnston c. Chief Constable of the Royal Ulster Constabulary*, (causa 222/84)

CGCE, sent. 17 dicembre 1970, *Internationale Handelsgesellschaft mbH c. Einfuhr- und Vorratsstelle für Getreide und Futtermittel* (causa C- 11/70)

CGCE, sent. 18 giungo 1991, *Elliniki Radiophonia Tiléorassi AE c. Dimotiki Etairia Pliroforissis e Sotirios Kouvelas (ERT)* (causa C. 260/89)

CGCE, sent. 21 febbraio 1960, *Geitling et al. c. Alta Autorità della CECA* (cause riunite C-16, 17, 18/59)

CGCE, sent. 21 settembre 1989, *Hoechst AG c. Commissione delle Comunità europee* (cause riunite 46/87 e 227/88)

CGCE, sent. 4 febbraio 1959, *Friesrich Stork et Co. c. Alta Autorità della CECA* (causa C-1/58)

CGCE, sent. 5 febbraio 1963, *Nv Algemene Transport – en expeditie onderneming Van Gen en Loos c. Amministrazione olandese delle imposte* (causa C-26/62)

CGCE, sent. 20 maggio 2003, *Österreichischer Rundfunk e altri* (cause riunite C-465/00, C-138/01 e C-139/120)

*Corte di Giustizia dell'Unione Europea (CGUE)*

CGUE, Conclusioni dell'AG Cruz Villalòn del 12 dicembre 2013, *Digital Rights Ireland* (causa C-293/12)

CGUE, Conclusioni dell'AG D. Ruiz-Jarabo Colomer del 22 dicembre 2008, *College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer* (C-553/07)

CGUE, Conclusioni dell'AG Henrik Saugmandsgaard Øe nelle sue conclusioni del 3 maggio 2018, *Ministerio Fiscal* (causa C-207/16)

CGUE, Conclusioni dell'AG Niilo Jääskinen, 25 giugno 2013, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González* (causa C-131/12), § 133.

CGUE, domanda di pronuncia pregiudiziale proposta dall'*Investigatory Powers Tribunal*, Londra (Regno Unito) del 31 ottobre 2017, *Privacy International/Secretary of State for Foreign and Commonwealth Affairs e a.* (causa C-623/17)

CGUE, domanda di pronuncia pregiudiziale proposta dalla *Cour constitutionnelle* (Belgio) il 2 agosto 2018, – *Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX c. Conseil des ministres,* (causa C- 520/18)

CGUE, domanda di pronuncia pregiudiziale proposta dalla High Court of Ireland l'11 giugno 2012 - *Digital Rights Ireland Ltd/Minister for*

*Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Sìochána, Ireland and the Attorney General* (causa C-293/12)

CGUE, domanda pregiudiziale, *Data Protection Commissioner c. Facebook Ireland Limited, Maximilian Schrems* (causa C-311/18)

CGUE, domanda pregiudiziale, *Google Inc. c. Commission nationale de l'informatique et des libertés* (CNIL)(causa C-507/17)

CGUE, *Irlanda c. Parlamento europeo e Consiglio dell'Unione europea* (causa C-301/06)

CGUE, parere 1/15 (Accordo PNR EU-Canada) del 26 luglio 2017

CGUE, sent. 11 febbraio 1971, *Norddeutsches Vieh-und Fleischkontor v. Hauptzollamt Hamburg St Annen* ( causa C-39/70)

CGUE, sent. 13 dicembre 1979, *Liselotte Hauer c. Land Rheinland-Pfalz* (causa C-44/79)

CGUE, sent. 14 febbraio 2019, *Sergejs Buivids* (causa C-345/17

CGUE, sent. 14 settembre 2000, *Fisher* (causa C-369/98)

CGUE, sent. 16 dicembre 2008, *Heinz Huber c. Bundesrepublik Deutschland* (causa C-524/06)

CGUE, sent. 16 luglio 2015, *ClientEarth e Pesticide Action Network Europe (PAN Europe) c. Autorità europea per la sicurezza alimentare (EFSA)* (causa C-615/13)

CGUE, sent. 16 ottobre 2012, *Commissione europea c. Repubblica d'Austria* (C-614/10)

CGUE, sent. 17 luglio 2014, *YS e a.* (cause riunite C-141/12 e C-372/12)

CGUE, sent. 19 ottobre 2016, *Patrick Breyer c. Bundesrepublik Deutschland* (causa C-582/14)

CGUE, sent. 20 dicembre 2017, *Global Starnet Ltd c. Ministero dell'Economia e delle Finanze e Amministrazione Autonoma Monopoli di Stato* (causa C-322/16)

CGUE, sent. 20 maggio 2003, *Österreichischer Rundfunk e a.* (cause C-465/00, C-138/01)

CGUE, sent. 21 dicembre 2011, *Danske Svineproducenter v. Justitsministeriet* (causa C-316/10)

CGUE, sent. 21 dicembre 2016, *Tele2 Sverige AB contro Post- och telestyrelsen e Secretary of State for the Home Department contro Tom Watson e a.* (cause riunite C-03/15 e C-698/15)

CGUE, sent. 24 novembre 2011, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) / Administración del Estado* (cause riunite C-468/10, C-469/10)

CGUE, sent. 24 novembre 2011, *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, (causa C-70/10)

CGUE, sent. 24 settembre 2019, *Google LLC, succeduta alla Google Inc. c. Commission nationale de l'informatique et des libertés (CNIL)* (causa C-507/17)

CGUE, sent. 26 dicembre 2008, *Tietosuojavaltuutettu contro Satakunnan Markkinapörssi Oy e Satamedia Oy* (causa C-73/07).

CGUE, sent. 26 novembre 2009, *Commissione c. Grecia* (causa C-211/09)

CGUE, sent. 26 novembre 2009, *Commissione c. Irlanda* (causa C-202/09)

CGUE, sent. 29 gennaio 2008, *Productores de Música de España (Promusicae) contro Telefónica de España SAU* (causa C-275/06)

CGUE, sent. 29 luglio 2010, *Commissione/Austria* (causa C-189/2009)

CGUE, sent. 30 maggio 2013, *Commissione/Svezia* (causa C-270/2011)

CGUE, sent. 30 maggio 2013, *Worten – Equipamentos para o Lar SA c. Autoridade para as Condições de Trabalho (ACT)* (causa 342/12)

CGUE, sent. 31 gennaio 1978, *Fratelli Zerbone Snc v. Amministrazione delle finanze dello Stato* (causa C-94/77)

CGUE, sent. 4 febbraio 2010, *Commissione c. Svezia* (causa C-185/09)

CGUE, sent. 4 maggio 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde contro Rīgas pašvaldības SIA "Rīgas satiksme"* (causa C-13/16)

CGUE, sent. 6 novembre 2003, *Lindqvist* (causa C-101/01)

CGUE, sent. 7 maggio 2009, *College van burgemeester en wethouders van Rotterdam c. M. E. E. Rijkeboer* (causa C-553/07)

CGUE, sent. 8 aprile 2014, *Commissione europea c. Ungheria* (causa C-228/12)

CGUE, sent. 8 aprile 2014, *Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.* (cause riunite C-293/12 e C-594/12)

CGUE, sent. 8 novembre 2007, *The Bavarian Lager Co. Ltd c. Commissione delle Comunità europee* (T-194/04)

CGUE, sent. 8 ottobre 2018, *Ministerio Fiscal* (causa C-207/16)

CGUE, sent. 9 marzo 2010, *Commissione europea c. Repubblica federale di Germania* (C-518/07)

CGUE, sent. del 16 dicembre 2008, *Tietosuojavaltuutettu contro Satakunnan Markkinapörssi Oy e Satamedia Oy* (causa C-73/07)

CGUE, sent. del 6 ottobre 2015, *Maximillian Schrems c. Data Protection Commissioner* (causa C-362/14)

CGUE, sent., 27 settembre 2017, *Peter Puškár c. Finančné riaditeľstvo Slovenskej republiky e Kriminálny úrad finančnej správy* (causa C-73/16)

*Corte Europea dei Diritti dell'Uomo (Corte EDU)*

Corte EDU, sent. 10 febbraio 2009, *Iordachi c. Moldavia* (n. 25198/02 )

Corte EDU, sent. 11 luglio 2002, *Christine Goodwin c. Regno Unito* (n. 28957/95)

Corte EDU, sent. 15 marzo 2015, *Lambert c. Francia* (46043/14)

Corte EDU, sent. 16 febbraio 2000, *Amann c. Svizzera* (n. 27798/95)

Corte EDU, sent. 17 luglio 2003, *Perry c. Regno Unito* (n. 63737/00)

Corte EDU, sent. 19 febbraio 1998, *Guerra c. Italia* (n. 14967/89)

Corte EDU, sent. 19 giugno 2017, *M.M. c. Paesi Bassi* (n. 15993/09)

Corte EDU, sent. 2 agosto 1984, *Malone c. Regno Unito* (n. 8691/79)

Corte EDU, sent. 23 settembre 1998, *McLeod c. Regno Unito* (n. 24755/94 )

Corte EDU, sent. 24 febbraio 1995, *Antony e Margaret McMichael c. Regno Unito* (n. 16424/90)

Corte EDU, sent. 25 marzo 1992, *B. c. Francia* (n. 13343/87)

Corte EDU, sent. 25 marzo 1998, *Kopp c. Svizzera* (n. 23224/94)

Corte EDU, sent. 25 ottobre 1986, *Rees c. Regno Unito* (n. 9532/81)

Corte EDU, sent. 25 settembre 2001, *P.G. e J.H. c. Regno Unito* (n. 44787/98)

Corte EDU, sent. 25 settembre 2012, *Godelli c. Italia* (n. 33783/09)

Corte EDU, sent. 26 marzo 1987, *Leander c. Svezia* (n. 9248/81)

Corte EDU, sent. 27 settembre 1990, *Cossey c. Regno Unito* (n. 10843/84)

Corte EDU, sent. 28 gennaio 2000, *McGinley & Egan c. Regno Unito* (nn. 21825/93 e 23424/94)

Corte EDU, sent. 28 gennaio 2003, *Peck c. Regno Unito* (n. 44647/98)

Corte EDU, sent. 3 aprile 2007, *Copland c. Regno Unito* (n. 62617/00)

Corte EDU, sent. 4 dicembre 2015, *Zakharov c/o Russia* (n. 47143/06)

Corte EDU, sent. 4 maggio 2000, *Rotaru c. Romania* (n. 28341/95)

Corte EDU, sent. 6 settembre 1978, *Klass c. Germania* (n. 5029/71)

Corte EDU, sent. 7 luglio 1989,*Gaskin c. Regno Unito* (n. 10454/83)

Corte EDU, sent. 9 gennaio 2001, *Natoli c. Italia* (n. 26161/95)

## Fonti normative e lavori preparatori

*Fonti italiane*

d.lgs. 11 maggio 1999, n. 135, recante *Disposizioni integrative della legge 31 dicembre 1996, n. 675, sul trattamento di dati sensibili da parte dei soggetti pubblici*

d.lgs. 13 maggio 1998, n. 171, recante *Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attività giornalistica*

d.lgs. 26 febbraio 1999, n. 51, recante *Disposizioni integrative e correttive della legge 31 dicembre 1996, n. 675) concernenti il personale dell'ufficio del Garante per la protezione dei dati personali*

d.lgs. 28 luglio 1997, n. 255, recante *Disposizioni integrative e correttive della legge 31 dicembre 1996) n. 675, in materia di notificazione dei trattamenti di dati personali a norma dell'articolo 1, comma 1) lettera f), della legge 31 dicembre 1996, n. 676*

D.lgs. 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali.*

d.lgs. 30 luglio 1999, n. 281, recante *Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica*

d.lgs. 30 luglio 1999, n. 282, recante *Disposizioni per garantire la riservatezza dei dati personali in ambito sanitario.*

d.lgs. 6 novembre 1998, n. 389, recante *Disposizioni in materia di trattamento di dati particolari da parte di soggetti pubblici*;

d.lgs. 8 maggio 1998, n. 135, recante *Disposizioni in materia di trattamento di dati particolari da parte di soggetti pubblici*

d.lgs. 9 maggio 1997, n. 123, recante *Disposizioni correttive ed integrative della legge 31 dicembre 1996) n. 675) in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*

legge 20 novembre 2017, n. 167 – «*Disposizioni per l'adeguamento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea – Legge europea 2017*»

legge 25 ottobre 2017, n. 163 – «*Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2016-2017*»

Legge n. 675 del 31 dicembre 1996, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*

*Fonti europee*

Decisione n. 1247/2002/CE del Parlamento Europeo, del Consiglio e della Commissione del 1º luglio 2002 relativa allo statuto e alle condizioni generali d'esercizio delle funzioni di garante europeo della protezione dei dati

Dichiarazione n. 21 allegata al Trattato di Lisbona in Dichiarazioni allegate all'atto finale della Conferenza intergovernativa che ha adottato il Trattato di Lisbona, 13 dicembre 2007

Direttiva (UE) 2016/680 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 e che abroga la decisione quadro 2008/977/GAI del Consiglio

Direttiva (UE) 2016/681 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 nei confronti dei reati di terrorismo e dei reati gravi

Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE

Direttiva 2002/58 del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)

Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006 , riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE

Direttiva 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

*Draft Chater of Fundamental Rights of the European Union,* CHARTE 4370/00 CONTRIB 233, Bruxelles, 15 giugno 2000

Progetto presentato dal Francia, Inghilterra, Regno Unito e Irlanda, *Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detect*, doc. 8958/04, 20 dicembre 2004

Proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche) (Procedimento 2017/0003/COD - COM (2017) 10).

Proposta di Regolamento del Parlamento europeo e del Consiglio, relativo a un quadro applicabile alla libera circolazione dei dati non-personali nell'Unione europea del 13 settembre 2017

Proposta direttiva che instituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica (COM(2000) 393 def.)

Proposta direttiva relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica (COM(2000) 392 def.)

Proposta direttiva relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (COM(2000) 385 def.)

Proposta direttiva relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime (COM(2000) 384 def.)

Proposta direttiva relativa all'autorizzazione per le reti e i servizi di comunicazione elettronica (COM (2000) 386 def.)

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 (regolamento generale sulla protezione dei dati)

Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE

Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea

Regolamento 45/2001/CE del Parlamento europeo e del Consiglio, del 18 dicembre 2000, 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

Documenti

*Parlamento europea*

PE, *Recommendations from Parliament to the Commission and Council pursuant to paragraph 10 of the motion for a resolution concerning the principles which should form the basis of Community norms on the protection of the rights of the individual in the face of developing technical progress in the field of data processing*

PE, *Resolution of the European Parliament on the protection for the rights of the individual in the face of the technical progress in the field of automatic data processing*, 1979, GUCE C140/34;

PE, *Resolution of the European Parliament on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing*, 1975, GUCE 60/48;

PE, *Resolution of the European Parliament on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing*, 1976, GUCE C100/27

PE, *Resolution of the European Parliament on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing* 1982 GUCE C87/39

*Commissione delle Comunità europee*

CCE, *A four-year programme for the development of informatics in the Community*, commissionato al Consiglio dalla Commissione, 1976 (COM(76) 534 def

CCE, *Communication by the Commission of the European Communities concerning a Community policy for data processing*, in *Information – memo*, P-63/73 disponibile in *Archive od European Integration*, cit.

CCE, *Raccomandazione della Commissione del 29 luglio 1981 concernente una convenzione del Consiglio d'Europa sulla protezione delle persone per quanto riguarda l'elaborazione automatica dei dati a carattere personale (81 /679/CEE),* GUCE L246/31

CCE, *Relazione della Commissione sulla salvaguardia dei diritti fondamentali*, in *Gazzetta Ufficiale delle Comunità europee,* 5/76, COM(76) 37 def.

CCE, *Scientific and technological policy program*, commissionato al Consiglio dalla Commissione il 1° agosto 1973 (COM(73)1250, 25 luglio 29173, *Gazzetta Ufficiale delle Comunità Europee*, Supplemento n. 14/73)

CCE, *Una sfida per l'Europa*, in *Gazzetta Ufficiale delle Comunità europee*, supplemento 1/76

CCE, *Community policy on data processing* (Comunicazione della Commissione e del Consiglio). SEC(73) 43 def., Bruxelles

CCE, *Comunicazione della Commissione concernente la protezione delle persone per quanto riguarda il trattamento dei dati personali nella Comunità e la sicurezza dei sistemi d'informazione*, 24 settembre 1990, Bruxelles (COM(90) 314 def.– SYN 287 e 288)

CCE, *Rapporto sull'Unione Europea*, in *Gazzetta Ufficiale delle Comunità europee*, 5/75

Commissione delle Comunità europee, *The European Community and data processing: Government development aids permitted*, in *Information-Competition*, n. 21

*Commissione europea*

Comunicazione della Commissione al Consiglio e al Parlamento europeo, *Valutazioni dell'applicazione della Direttiva sulla conservazione dei dati (Direttiva 2006/24/CE),* COM (2011)

Commissione europea, Agenda digitale europea (COM(2010) 245 def.)

Commissione europea, *Comunicazione della Commissione al Parlamento Europeo e al Consiglio - Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini* (COM (2009) 262), 6 giugno 2009

Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni – Salvaguardare la privacy in un mondo interconnesso. Un quadro europeo della protezione dei dati per il XXI secolo* (COM (2012) 9 def.), 25 gennaio 2012

Commissione europea, *Per l'affermazione dei diritti fondamentali nell'Unione europea – Relazione del gruppo di esperti in materia di diritti fondamentali*, febbraio 1999

Commissione europea, piano d'azione della Commissione per l'attuazione del programma di Stoccolma (COM(2010) 171 def.)

Commissione europea, *Proposta di direttiva del Parlamento e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (presentata dalla Commissione)* (COM(2000) 385 def.

Commissione europea, *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.), 25 gennaio 2012.

Commissione europea, strategia Europa 2020 dell'UE (COM(2010) 2020 def.).

Comunicazione della Commissione al Parlamento europeo, al Consiglio, la Comitato economico e sociale europeo e al Comitato delle regioni, *Un approccio globale alla protezione dei dati personali nell'Unione Europea*, Bruxelles, 4 novembre 2010

Commissione europea, relazione della Commissione al Consiglio e al Parlamento europeo, *Valutazioni dell'applicazione della Direttiva sulla conservazione dei dati (Direttiva 2006/24/CE)*

*Consiglio dell'Unione europea*

Consiglio dell'UE, *Progetto di decisione quadro sulla conservazione dei dati trattati e memorizzati nel quadro della fornitura di servizi di comunicazioni elettroniche accessibili al pubblico o dei dati sulle reti pubbliche di comunicazione a fini di prevenzione, ricerca,*

*accertamento e perseguimento della criminalità e dei reati, compreso il terrorismo*, doc. 15098/04, 23 novembre 2004

Consiglio dell'UE, *Progetto di decisione quadro sulla conservazione dei dati trattati e memorizzati nel quadro della fornitura di servizi di comunicazioni elettroniche accessibili al pubblico o dei dati sulle reti pubbliche di comunicazione a fini di prevenzione, ricerca, accertamento e perseguimento della criminalità e dei reati, compreso il terrorismo - Base giuridica*, doc. 7688/05, 5 aprile 2005

Consiglio dell'UE, *Dichiarazione sulla lotta al terrorismo*, 25 marzo 2004.

*Consiglio d'Europa*

Consiglio d'Europa, *Council of Europe Conference of Ministers on Freedom of Expression and Democracy in the Digital Age*, 2013 (MCM(2013)007)

Consiglio d'Europa, nella raccomandazione CM/Rec(2010)13 del Comitato dei Ministri agli Stati Membri sulla protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione, adottata dal Comitato dei Ministri il 23 novembre 2010 in occasione del 109mo incontro dei Rappresentanti dei Ministri

*Gruppo Articolo 29*

Gruppo Articolo 29, Gruppo di lavoro "Polizia e Giustizia", *The Future of Privacy – Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data* (WP 168) del 1 dicembre 2009.

Gruppo Articolo 29, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679* (WP248 rev.1) del 4 ottobre 2017

Gruppo Articolo 29, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679* (WP248 rev.1) del 4 ottobre 2017

Gruppo Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679* (WP 251 rev. 01) del 6 febbraio 2018

Gruppo Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679* (WP251 rev.1) del 6 febbraio 2018

Gruppo Articolo 29, *Opinion 02/2012 on facial recognition in online and mobile services* (WP192) del 22 marzo 2012

Gruppo Articolo 29, *Opinion 02/2013 on apps on smart devices* (WP202) del 27 febbraio 2013

Gruppo Articolo 29, *Opinion 05/2012 on Cloud Computing* (WP196) del 1 luglio 2012

Gruppo Articolo 29, *Opinion 05/2013 on Smart Borders* (WP206) del 6 giugno 2013

Gruppo Articolo 29, *Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force* (WP209) del 4 dicembre 2013

Gruppo Articolo 29, *Opinion 1/2008 on data protection issues related to search engines* (WP138) del 4 aprile 2008

Gruppo Articolo 29, *Opinion 13/2011 on Geolocation services on smart mobile devices* (WP185) del 6 maggio 2011

Gruppo Articolo 29, *Opinion 2/2010 on online behavioral advertising* (WP171) del 22 giugno 2010

Gruppo Articolo 29, *Opinion 3/2012 on developments in biometric technologies* (WP193) del 27 aprile 2012

Gruppo Articolo 29, *Opinion 5/2009 on online social networking* (WP163) del 12 giugno 2009

Gruppo Articolo 29, *Opinion 8/2014 on the on Recent Developments on the Internet of Things* (WP223) del 16 settembre 2014

Gruppo Articolo 29, *Parere 05/2014 sulle tecniche di anonimizzazione*, (WP216) del 10 aprile 2014

Gruppo Articolo 29, *Parere 3/2013 sulla limitazione delle finalità* (WP203) del 2 aprile 2013

Gruppo Articolo 29, *Parere 4/2007 sul concetto di dato* personale (WP136) del 20 giugno 2007

Gruppo Articolo 29, *Parere 4/2007 sul concetto di dato personale*, (WP136) del 20 giugno 2007

Gruppo Articolo 29, *Parere 5/2014 sulle tecniche di anonimizzazione* (WP216) 10 aprile 2014

Gruppo Articolo 29, *Raccomandazione 4/99 concernente l'inclusione del diritto fondamentale alla protezione dei dati personali nella Carta europea dei diritti fondamentali* (WP26) del 7 settembre 1999

Gruppo Articolo 29, *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*, (WP221) del 16 settembre 2014

Gruppo Articolo 29, *Statement on the role of a risk-based approach in data protection legal frameworks* (WP218) del 30 maggio 2014

Gruppo Articolo 29, *The Future of Privacy: Joint contribution to the Consultation in the European Commission on the legal framework for the fundamental right to protection of personal data* (WP168) del 1° dicembre 2009

*Garante Europeo per la protezione dei dati personali*

EDPS, *EDPS Opinion on coherent enfaorcement of fundamental rights in the age of big data,* parere del 23 settembre 2016, n. 8,

EDPS, *EDPS Opinion on coherent enforcement of fundamental rights in the age of big data,* parere 8/2016

EDPS, *EDPS Opinion on online manipulation and personal data*, parere 3/2018

EDPS, *Meeting the challenges of big data A call for transparency, user control, data protection by design and accountability,* parere 7/2015

EDPS, *Opinion 5/2018 – Preliminary Opinion on privacy by design,* 31 maggio 2018

EDPS, *Verso una nuova etica digitale. Dati, dignità e tecnologia*, parere n. 4, 11 settembre 2015

*Altro*

Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale istituto dalla Commissione europea nel giugno 2018, *Una definizione di IA: principali capacità e discipline* (*definizione elaborata ai fini dei documenti del gruppo*), aprile 2019

Gruppo indipendenti di esperti ad alto livello sull'intelligenza artificiale, istituito dalla Commissione europea nel giugno 2018, *Orientamenti etici per un IA affidabile*, del 8 aprile 2019

OECD, *Exploring the economics of personal data: a Survey of Methodologies for Measuring Monetary Value*, del 2 aprile 2013