


UNIVERSITÀ DEGLI STUDI DI MACERATA

CORSO DI DOTTORATO DI RICERCA IN

SCIENZE GIURIDICHE

CICLO XXXIV

LA DISCIPLINA EUROPEA DEI DATI:

DALLA PROTEZIONE ALLA *GOVERNANCE*

SUPERVISORE DI TESI

Chiar.mo Prof. Simone Calzolaio

DOTTORANDO

Dott. Stefano Torregiani

COORDINATORE

Chiar.mo Prof. Massimo Meccarelli

ANNO 2022

INDICE

INTRODUZIONE 4

CAPITOLO I

DAL DATO PERSONALE AL DATO NON PERSONALE: EVOLUZIONE GIURIDICA DELL'ORDINAMENTO EUROPEO

1. Introduzione 14

2. L'esperienza tedesca e l'affermazione giurisprudenziale del diritto alla autodeterminazione informativa 16

3. Il panorama internazionale in materia di protezione dei dati 24

4. Il consolidamento della disciplina a livello comunitario: l'epoca delle direttive 31

5. La costituzionalizzazione del diritto alla protezione dei dati personali: dalla Carta europea dei diritti fondamentali al riconoscimento da parte della Corte di giustizia dell'Unione europea 41

6. La normativa vigente: il Regolamento (UE) 2016/679 e il Regolamento (UE) 2018/1807 (*cenni*) 62

CAPITOLO II

LA LIBERA CIRCOLAZIONE DEI DATI TRA IL REGOLAMENTO (UE) 2016/679 E IL REGOLAMENTO (UE) 2018/1807

1. La circolazione dei dati come terreno di confronto 76

2. L'Unione tra mercato dei dati europeo e *data localization* 78

3. La circolazione dei dati personali 88

3.1 All'interno dell'Unione europea 88

3.2 Al di fuori dell'Unione europea 91

4. La circolazione dei dati non personali 97

4.1 Il divieto degli obblighi di localizzazione 98

4.2 Una nuova portabilità autoregolamentata: dalla "*portability*" al "*porting*" 112

5. Tessere mancanti nel mosaico regolamentare europeo? 116

CAPITOLO III

LA QUALIFICAZIONE DEL "DATO" SECONDO I CRITERI DELL'ORDINAMENTO EUROPEO

1. Introduzione 122

2. La definizione ampia di dato personale 124

2.1 Le articolazioni del dato personale 131

2.2 Gli elementi costitutivi del dato personale 145

3. Il dato non personale 170

3.1 Il dato anonimizzato 174

3.1.1 Anonimizzazione e rischio di re-identificazione 174

3.1.2 Il design del trattamento residuo in chiave contestuale .180

3.2 Il dato industriale e la questione della proprietà 187

3.2.1 Le soluzioni *de iure condito*: le normative vigenti 190

3.2.2 La regolazione della *data economy* tra proprietà ed accesso 193

4. Dagli insiemi di dati misti al "*Data by Design*" 200

5. Verso la regolamentazione di un sistema integrato di gestione dei dati 206

CAPITOLO IV

IL NUOVO MODELLO EUROPEO PER LA *GOVERNANCE* DEI DATI

1. Introduzione 213

2. Un nuovo modello "europeo" di *data governance* basato sulla condivisione dei dati 217

3. Il potenziale impatto delle nuove normative sul diritto europeo dei dati 226

3.1 Il riutilizzo dei dati “protetti” detenuti dagli enti pubblici e la seconda vita dei dati non personali 232

3.2 Profili soggettivi del *data sharing* nel DGA 241

3.2.1 Gli attori necessari e la persistenza dei problemi di qualificazione giuridica dei titolari dei dati 242

3.2.2 Il ruolo caratterizzante dell’intermediario di dati nell’impianto europeo 247

4. Spazio comune europeo di dati: *interdependence model versus independence model* 254

CONCLUSIONI 267

BIBLIOGRAFIA 275

INTRODUZIONE

Il termine *datafication* (o datificazione)[1] descrive il processo di trasformazione delle interazioni sociali in dati digitali quantificabili al fine rendere possibile la loro classificazione e la loro analisi.[2] In tal senso, la datificazione costituisce l'evoluzione della digitalizzazione: se quest'ultima aveva permesso di trasferire le informazioni dal mondo analogico a quello digitale, continuando però a trattare il loro contenuto semantico in maniera scissa dal contenitore sintattico (il dato), con la fusione tra dato e informazione garantita dalla datificazione viene agevolata una analisi più avanzata in quanto capace di individuare modelli ricorrenti e corrispondenze nascoste anche nell'ambito di grandi insiemi di dati.[3] A tale fenomeno è, fondamentalmente, imputabile la crescita esponenziale, non solo nella quantità, ma soprattutto nella rilevanza che ha contraddistinto i dati, divenuti oramai una risorsa digitale essenziale per la conduzione di qualsiasi attività pubblica o privata.[4]

Un cambiamento di simile portata ha inevitabilmente alterato gli equilibri economici e geopolitici preesistenti, facendo confluire maggiore potere nelle mani di quegli attori, pubblici o privati, che

[1] Il termine viene ricondotto all'opera di MAYER-SCHOENBERGER V., CUKIER K., *Big Data. A Revolution that will transform how we live, work, and think*, London, John Murray Publishers, 2013.

[2] VAN DIJCK J., *Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology*, in *Surveillance and Society*, Vol. 12, No. 2, 2014, pp. 197 e ss.; MARTONI M., *Datificazione dei nativi digitali. Una prima ricognizione e alcune brevi note sull'educazione alla cittadinanza digitale*, in *federalismi.it*, n. 1/2020, pp. 119 e ss.

[3] MAI J.-E., *Big data privacy: The datafication of personal information*, in *The Information Society*, Vol. 32, No. 3, 2016, pp. 192 e ss.; OROFINO M., *Trattamento dei dati personali e libertà di espressione e di informazione*, in CALIFANO L., COLAPIETRO C. (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, Napoli, 2017, pp. 508- 538. In virtù di quanto affermato, nella presente tesi le nozioni di dato e informazione verranno impiegate come termini aventi il medesimo significato, salvo diversa specificazione.

[4] SURBLYTE G., *Data as a Digital Resource*, in *Max Planck Institute for Innovation & Competition Research Paper No. 16-12*, 2016.

per primi erano riusciti ad assicurarsi l'accesso a questo nuovo e prezioso asset. Per contro, l'inerzia iniziale in tema di sviluppo delle tecnologie digitali è costata cara all'Unione europea: potenze come Stati Uniti d'America e Repubblica Popolare Cinese si trovano ora in una posizione di manifesta superiorità tecnica, difficilmente raggiungibile dal vecchio continente nel breve periodo.[5] Pertanto, l'Unione ha deciso di intervenire, *in primis*, a livello normativo al fine di arrestare il processo di graduale erosione della propria sovranità causato dal mancato sfruttamento dei dati. In ragione della carenza di infrastrutture e competenze negli Stati membri, il ricorso ad atti di diritto derivato è stato identificato come la strada principale da intraprendere, in quanto capace di tamponare la fuoriuscita di dati preziosi dal perimetro virtuale europeo in maniera tanto immediata quanto, in linea teorica, efficace.

L'intensificazione della produzione di provvedimenti, di stampo normativo e istituzionale, specificamente dedicati alla tutela e al corretto sfruttamento dei dati – figlia della datificazione e degli effetti che ne sono conseguiti – sembra indicare che, in seno agli ordinamenti europeo e degli Stati membri dell'Unione, il diritto dei dati, o *data law*, si stia affermando quale branca speciale del diritto, rispondente a principi e regole propri e, in parte, autonomi. Il quadro normativo attualmente vigente in Europa si basa sulla fondamentale distinzione tra dati personali, in quanto riguardanti una persona fisica identificata o identificabile, e quelli non personali che, per converso, includono tutte le informazioni non rientranti nella prima categoria. A questa distinzione di fondo fanno riferimento i due principali regolamenti in materia: da un lato, il Regolamento (UE) 2016/679

[5] Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) (SWD(2020) 295 final), p. 1.

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e, dall'altro, il Regolamento (UE) 2018/1807 relativo a un quadro applicabile alla libera circolazione dei dati non personali. La disamina del sistema normativo europeo proposta nell'ambito del presente lavoro tende a mostrare un forte squilibrio tra questi due poli: il baricentro della disciplina è pesantemente spostato verso la normazione dei dati a carattere personale in ragione della qualifica di diritto di rango fondamentale che la protezione di queste informazioni ha assunto nell'ordinamento europeo. Conseguentemente, anche la dottrina pubblicistica continentale ha preso la medesima piega, incentrando i propri studi sull'esigenza di protezione dell'individuo dalle conseguenze negative che possono derivare dall'utilizzo (anche lecito) delle informazioni che lo riguardano. Sull'altro versante, invece, i dati non personali sono stati prevalentemente oggetto di approfondimento da parte di esperti afferenti ai settori commerciale, economico e privatistico, con particolare riferimento all'ambito della tutela della proprietà intellettuale.

Le ragioni alla base del consolidamento di tale quadro regolamentare e dottrinale sono riconducibili alla peculiare evoluzione del diritto dei dati in territorio europeo, dove gli strascichi del secondo conflitto mondiale hanno favorito lo sviluppo di un'impostazione, prima giurisprudenziale, poi normativa, intenta a non sacrificare gli interessi individuali di fronte al crescente utilizzo degli strumenti di trattamento automatizzato dei dati personali da parte delle autorità pubbliche. Tuttavia, i cambiamenti radicali che nell'ultimo decennio hanno interessato il settore delle tecnologie dell'informazione e della comunicazione sollecitano un

mutamento nell'approccio allo studio della materia.[6] Le attuali capacità di analisi dei dati dimostrate dalle macchine hanno portato alla luce due aspetti di preminente rilevanza. In primo luogo, la distinzione su cui è stato edificato il diritto europeo dei dati è molto meno chiara di quanto la legge lasci presuppore: la qualificazione di una informazione come personale o meno è pesantemente influenzata dal punto di osservazione che assume l'interprete e dagli elementi pertinenti che egli prende in considerazione in sede di valutazione. In secondo luogo, l'utilizzo degli strumenti moderni ha oramai dimostrato che ripercussioni significative sulla società e sulle persone che vi appartengono non derivano più solo ed esclusivamente dal trattamento di informazioni a carattere personale. Con la diffusione dei *Big Data*, l'impiego di qualsiasi tipo di informazione, anche non personale, assume un valore nuovo, poiché contribuisce a produrre risultanze sulla base delle quali il mondo in cui viviamo viene plasmato e modificato.[7] Pertanto, sebbene sia comprensibile e assolutamente condivisibile la scelta di orientare le prime regole e i primi studi sui profili che comportano rischi più immediati per la persona fisica, sembra ora arrivato il momento di dedicare alcune riflessioni anche ad altre dimensioni inerenti al diritto dei dati.

Da tali considerazioni, essenzialmente, sono nate le domande che hanno guidato la redazione dell'elaborato, il quale si propone di osservare il sistema europeo di regolazione del trattamento delle informazioni adottando una prospettiva tesa ad includere altri interessi di rilievo costituzionale, prescindendo dalla considerazione del dato personale come unico fattore da presidiare per realizzare un

[6] SCHERMER B., *The limits of privacy in automated profiling and data mining*, in *Computer law & security review* 27, 2011, 45 ss.
[7] Commission nationale de l'informatique et des libertés (CNIL), *How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence*, 2017.

ordinamento che protegga efficacemente i valori fondamentali europei. In particolare, la ricerca è stata sviluppata con l'obiettivo di valutare se il quadro regolamentare europeo di *data law* attualmente in vigore sia idoneo a soddisfare anche esigenze diverse dalla tutela dell'individuo, fra le quali spiccano quelle – tra loro connesse – di sovranità e di competitività industriale, individuate dalle stesse istituzioni continentali come fini da perseguire per mezzo di opportuni interventi normativi. In altri termini, si tratta di comprendere se il sistema binario impostato dal legislatore europeo sia in armonia o, al contrario, entri in collisione, con le finalità che il legislatore medesimo vorrebbe raggiungere.

Invero, il mantenimento della sovranità dell'Unione europea e degli Stati membri passa anche attraverso la realizzazione di un comparto industriale all'avanguardia, capace di reggere la competizione con le grandi compagnie extraeuropee. Nello specifico, la *smart manufacturing*,[8] specie a seguito dell'osservazione empirica maturata nel corso dello svolgimento della ricerca dottorale, rappresenta un osservatorio privilegiato per comprendere le ricadute che le regole volte a disciplinare la gestione dei dati possono avere sullo sviluppo dell'industria continentale, in quanto, differentemente da quanto accade in altri contesti, la stragrande maggioranza delle informazioni gestite nell'ambito del ciclo produttivo manifatturiero, in particolare se automatizzato, non hanno alcun legame con persone

[8] La nozione di *smart manufacturing* adottata ai fini del presente studio coincide con quella concepita dallo Smart Manufacturing Coordinating Committee (SMCC), entità creata dal Technical Management Board (TMB) della International Organization for Standardization (ISO) al fine di coordinare le attività relative allo studio della manifattura intelligente. Tale definizione, approvata successivamente dalla ISO con la Risoluzione 31/2019, descrive la *smart manufacturing* come: "Manufacturing that improves its performance aspects with integrated and intelligent use of processes and resources in cyber, physical and human spheres to create and deliver products and services, which also collaborates with other domains within enterprises' value chains".

fisiche identificate o identificabili.[9] Difatti, con l'avvento della digitalizzazione , il settore industriale ha intrapreso un percorso di radicale trasformazione e rimeditazione di modelli e di processi produttivi consolidati. Oramai, ogni strumento, processo o metodo necessario alla costruzione della "fabbrica intelligente" si basa su un minimo comun denominatore: i dati.[10] Questi *asset* rappresentano un fattore imprescindibile per la *smart manufacturing* perché costituiscono la componente che rende possibile la realizzazione di sistemi ciber-fisici capaci di integrare i tradizionali sistemi fisici della manifattura con il ciberspazio: tecnologie come Big Data, *cloud computing*, *data anlytics* e robotica riescono a plasmare e ottimizzare la produzione, con dei risultati inimmaginabili fino a poco tempo fa.[11] In ragione di ciò, l'approccio all'utilizzo dei dati è mutato tanto profondamente quanto rapidamente in seno a qualsiasi realtà industriale.

Alla luce di tali premesse, la presente tesi muove da un'analisi *de iure condito* focalizzata sulle principali fonti normative in materia di dati ad oggi in vigore nell'ordinamento europeo, il Regolamento (UE) 2016/679 e il Regolamento (UE) 2018/1807, per concludere con le più recenti direttrici di riforma promosse dalle istituzioni europee, le quali sembrano confermare la necessità, ipotizzata in tesi, di procedere ad un riequilibrio dell'apparato normativo. A tale proposito, è opportuno premettere che, sebbene la disamina prenda in considerazione anche testi che al momento della redazione non hanno ancora acquisito carattere definitivo e che, pertanto, potranno

[9] KUSIAK A., *A Four-part Plan for Smart Manufacturing*, ISE Magazine, Vol. 49, No.7, 2017, pp. 43-47.
[10] ISO Smart Manufacturing Coordinating Committee, *White Paper on Smart Manufacturing*, 2021; KUSIAK A., *Fundamentals of smart manufacturing: A multi-thread perspective*, Annual Reviews in Control, Vol. 47, 2019, pp. 214-220.
[11] KUSIAK A., *Smart manufacturing*, International Journal of Production Research, 2018, pp. 508-517.

subire ulteriori modifiche nel corso dell'iter di approvazione, i documenti menzionati consentono sin da ora lo svolgimento di alcune considerazioni preliminari in merito ai nuovi orizzonti verso cui si sta dirigendo il sistema europeo di disciplina dei dati.

Da ultimo, si segnala che il vaglio degli atti di rango primario presi come riferimento ai fini dello svolgimento della ricerca è stato volutamente circoscritto ai soli provvedimenti aventi come oggetto principale una fra le dimensioni afferenti ai dati (nella fattispecie, trattamento, circolazione e *governance*). Tale scelta metodologica si fonda sulla funzione prodromica che il *data law* svolge nei confronti di tutte le discipline aventi come obiettivo la regolazione della tecnologia. Dipendendo quest'ultima, anzitutto, dalla trasmissione di dati, è evidente che qualsiasi tentativo di regolare la tecnologia passa, necessariamente, per la regolazione della gestione e della circolazione dei dati.[12]

Per quanto concerne la struttura, la tesi si articola in quattro distinti capitoli. Il primo di essi esamina l'evoluzione dell'ordinamento giuridico europeo dei dati, prendendo avvio dall'interpretazione che le corti nazionali europee hanno attribuito al concetto statunitense di privacy a partire dai primi anni Ottanta del secolo scorso. L'esposizione delle varie tappe susseguitesi sino alla vigenza della attuale normativa è stata condotta con l'obiettivo di favorire la comprensione dei motivi che hanno portato al consolidamento della protezione dei dati personali come diritto

[12] DELLA MORTE G., *Big Data e Protezione Internazionale Dei Diritti Umani. Regole e Conflitti*, in ARCARI M., MILANO E., TANZI. A. (diretta da), *La ricerca del diritto nella comunità internazionale*, Editoriale scientifica, Napoli, 2018, p. 135.

fondamentale e al conseguente sistema europeo “a due velocità” che relega i dati diversi da quelli personali a una posizione secondaria.

Il secondo capitolo si focalizza sul confronto fra il Regolamento (UE) 2016/679 e il Regolamento (UE) 2018/1807, ossia le due fonti normative di rango primario che definiscono la natura dei dati, rispettivamente, personali e non personali, nel tentativo di apprezzare le profonde differenze che li separano. La sezione in parola assume come termine di paragone fra le due discipline la particolare dimensione della circolazione dei dati, in quanto unico aspetto di rilievo cui il Regolamento (UE) 2018/1807 dedica le proprie prescrizioni. In tale contesto, la tesi mira ad approfondire il fenomeno della *data localization* che, traducendosi in un incremento di provvedimenti normativi e amministrativi volti a mantenere i dati all’interno di un determinato territorio, si pone in netta contrapposizione con il principio della libera circolazione dei dati.

Il terzo capitolo mette in luce l’aspetto cruciale della normativa: la distinzione tra dato personale e dato non personale. Attraverso la disamina delle sottocategorie di informazioni che rientrano nei due macro-insiemi principali e degli elementi che le contraddistinguono, si perviene ad una aumentata consapevolezza delle difficoltà insite nelle operazioni di separazione fra le due tipologie di informazioni e delle conseguenti problematiche di esatta individuazione dell’ambito di applicazione dei due Regolamenti.

Le formulazioni impiegate, specie quella di carattere negativo presente nel Regolamento (UE) 2018/1807, suggeriscono di procedere, in primo luogo, con l’esame dei singoli tasselli costituenti la definizione di dato personale al fine di cogliere le ripercussioni che il loro progressivo ampliamento, promosso dalla giurisprudenza e dal legislatore, potrebbe produrre nei confronti della classe contigua dei dati non personali. Conseguentemente, l’elaborato

proseguirà con lo studio di questa seconda tipologia di dati attraverso l'approfondimento delle due sottocategorie che la compongono: da un lato, il dato anonimizzato che, in ragione della sua originaria appartenenza alla classe dei dati personali, pone questioni particolarmente immediate e pressanti dal punto di vista della qualificazione giuridica, e, dall'altro lato, quella dei dati industriali, i quali stanno assumendo un valore nuovo nel contesto dell'attuale evoluzione tecnologica.

Il carente coordinamento fra le due fonti, che mina alla base la tenuta dell'intero impianto regolamentare, stimola alcune riflessioni *de iure condendo* per la definizione di un quadro normativo dotato di maggiore uniformità ed effettività, dove possa finalmente trovare spazio una qualificazione in chiave contestuale della natura del dato che assuma come punto di riferimento l'ambiente in cui opera il titolare del trattamento complessivamente considerato e non esclusivamente l'informazione presa in maniera isolata.

Da ultimo, il capitolo finale è dedicato all'esame delle proposte più recenti in tema di *data law*, per mezzo delle quali il legislatore sembra intenzionato a porre rimedio ad alcune delle criticità della disciplina. In particolare, l'obiettivo consiste nella realizzazione di un nuovo modello di *governance* dei dati dove la promozione della condivisione delle informazioni e l'introduzione di appositi diritti di accesso conducano alla creazione di uno "spazio comune europeo di dati", individuato quale strumento utile al fine di recuperare la competitività industriale e la sovranità che l'Unione europea ha perduto nel corso degli ultimi anni. Alla luce di tali ultime evoluzioni, si tenterà di comprendere se la direzione verso cui sta virando il diritto europeo dei dati contempla una rivalutazione e un riequilibrio dei dati non personali rispetto a quelli personali.

CAPITOLO I

DAL DATO PERSONALE AL DATO NON PERSONALE: EVOLUZIONE GIURIDICA DELL'ORDINAMENTO EUROPEO

Sommario: 1. Introduzione. 2. L'esperienza tedesca e l'affermazione giurisprudenziale del diritto alla autodeterminazione informativa. 3. Il panorama internazionale in materia di protezione dei dati. 4. Il consolidamento della disciplina a livello comunitario: l'epoca delle direttive. 5. La costituzionalizzazione del diritto alla protezione dei dati personali: dalla Carta europea dei diritti fondamentali al riconoscimento da parte della Corte di giustizia dell'Unione europea. 6. La normativa vigente: il Regolamento (UE) 2016/679 ed il Regolamento (UE) 2018/1807 (*cenni*).

1. Introduzione

Lo studio della fattispecie del dato non può prescindere da una preliminare analisi storico-giuridica degli eventi che hanno portato alla formazione della corrispondente disciplina all'interno dell'ordinamento europeo. L'obiettivo ultimo di questo capitolo risiede nella volontà di comprendere quale impatto l'evoluzione della giurisprudenza e delle normative nazionali e sovranazionali abbia avuto nei confronti della tecnica legislativa seguita dal legislatore dell'Unione, il quale ha completato questo percorso regolamentare optando per la formazione di una vera e propria spaccatura tra dati personali e dati non personali.

I paragrafi che seguono si soffermeranno sui principali passaggi della storia giuridica europea che hanno condotto all'affermazione di un diritto fondamentale alla tutela dei dati personali e, solamente in seguito, verrà dedicato apposito spazio al

confronto tra le due normative, quella concernente le informazioni che vantano un legame con una persona fisica e quella relativa alle informazioni che, al contrario, non si riferiscono ad alcun individuo. A tal fine, la presente disamina non approfondirà il tema del progressivo affrancamento del diritto alla protezione dei dati personali dall'originario diritto alla riservatezza, o *privacy*,[1] la cui nascita risale alla fine del XIX secolo.[2] Pertanto, l'apertura di questo percorso si collocherà in una fase temporale successiva, segnatamente, negli anni Settanta del Novecento in una Germania appena uscita sconfitta dal secondo conflitto mondiale ed ancora divisa. In questo frangente, cominciano a vedere la luce le prime normative e, soprattutto, le prime pronunce giurisprudenziali che teorizzano una protezione delle informazioni nuova e capace di garantire una tutela efficace di fronte all'avanzare della tecnologia informatica. Risale, difatti, a questo periodo l'adozione della prima disciplina organica in materia di dati all'interno del perimetro europeo, inaugurando così un cinquantennio di riforme e accesi dibattiti attorno ad una materia che, malgrado alcune normative a carattere prettamente settoriale, ha continuato a ruotare attorno all'asse costituito dai dati di natura personale.

L'analisi di questo cammino guiderà il lettore verso il più recente traguardo raggiunto dal legislatore europeo, consistente nell'adozione dei due regolamenti generali attualmente vigenti, uno riferito ai dati personali e l'altro ai dati non personali. Il confronto tra le soluzioni terminologiche e fra i principi inseriti nelle rispettive

[1] TIBERI G., Riservatezza e protezione dei dati personali, in CARTABIA M. (a cura di), *I diritti in azione*, Bologna, 2007, pp. 353 e ss.; CALIFANO L., *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, 2016, 9 e ss.; PARDOLESI R., *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in PARDOLESI R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003.
[2] WARREN S.D., BRANDEIS L.D., *The right to privacy*, *Harvard Law Review*, 1890.

normative costituisce un osservatorio ottimale per comprendere in che misura questo "strabismo" regolatorio rischi di avere ripercussioni sfavorevoli nei confronti dell'industria continentale, in particolare di quella manifatturiera.

2. L'esperienza tedesca e l'affermazione giurisprudenziale del diritto alla autodeterminazione informativa

Una delle tappe fondamentali della storia europea in materia di regolamentazione dei dati ha luogo nella Germania della Guerra fredda, in un'epoca in cui la pervasività del controllo del potere centrale nei confronti dei cittadini e l'incapacità di tenere al sicuro la propria sfera individuale aveva portato alla morte, alla cattura o alla deportazione di milioni di persone. Una precoce dimostrazione delle nefaste ripercussioni che possono derivare dall'esercizio del pubblico potere per mezzo di una tecnologia avulsa da qualsivoglia limite normativo si rinviene a partire dall'inizio degli anni Trenta quando le autorità pubbliche tedesche cominciarono ad utilizzare i primi macchinari di elaborazione dei dati basati su schede perforate al fine di effettuare un controllo diffuso e una catalogazione della cittadinanza.[3]

Il contesto della ripresa susseguente alla parentesi totalitaria, precisamente sul finire degli anni Sessanta e per tutta la decade successiva, si rivela particolarmente fertile per intraprendere una analitica discussione in merito al trattamento delle informazioni relative alle persone fisiche: ai primi interrogativi che la dottrina solleva con riguardo alla elaborazione di informazioni per mezzo di

[3] PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali, I, Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, P. 52 e ss.

sistemi automatizzati, fanno da contraltare i risultati prodotti dalle commissioni incaricate dai membri dei governi occidentali industrialmente più avanzati intenti ad illustrare le possibili evoluzioni dell'utilizzo da parte della pubblica amministrazione degli ultimi ritrovati della tecnologia dell'informazione.[4] Dal punto di vista legislativo, le istanze sociali di regolazione dei sistemi di analisi di dati si traducono per la prima volta in normativa nel Land dell'Assia, dove nel 1970 viene approvata la Legge sulla protezione dei dati dell'Assia (Hessisches Datenschutzgesetz) volta a disciplinare il trattamento dei dati personali nell'ambito del settore pubblico.[5] Questo intervento funge da apripista per tutte le altre normative europee che entreranno in vigore nel corso del medesimo decennio: prima la legge svedese (Datalag) nel 1973, poi un'altra legge tedesca (Bundesdatenschutzgesetz), questa volta adottata a livello federale, nel 1977 e infine quella francese (Loi informatique, fichiers et libertés) del 1978, ancora oggi in vigore. Nonostante i sistemi di analisi fossero ancora lontani dal livello di quelli moderni, queste discipline dimostrano un'apprezzabile lungimiranza, in quanto introducono alcuni fra i cardini su cui poggia la disciplina europea attualmente vigente: la presenza di una base legittima per il trattamento, la nomina di un responsabile per la protezione dei dati personali e la previsione di un'autorità di controllo facente funzione di garante. La comparsa in scena di numerose normative in un arco temporale così ristretto si inserisce a pieno titolo in quella corrente di rinnovamento dell'originario concetto di *privacy* che attraversa tutto l'Occidente a cavallo degli anni Settanta. Il comune bisogno di

[4] OECD, *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, in *OECD Digital Economy Papers*, No. 176, OECD Publishing, Paris, 2011, pp. 7 e ss.
[5] GONZALEZ FUSTER G., *The emergence of personal data protection as a fundamental right of the EU*, Springer, 2014.

innalzare un argine efficace all'ingresso delle nuove tecniche di analisi nella vita privata dei cittadini, se negli Stati Uniti aveva portato all'elaborazione della nozione di *informational privacy*,[6] in territorio continentale stava spingendo i singoli Stati verso il consolidamento della versione europea di tutela della *privacy*, dove alla libertà di carattere negativo di essere lasciati soli, si aggiunge una nuova dimensione dinamica e attiva, in ragione della quale all'individuo vengono riconosciuti poteri di controllo e di intervento quando sono trattate informazioni che lo riguardano.[7]

A tale proposito, un notevole impulso verso la concezione "dinamica" del diritto alla protezione dei dati personali come lo conosciamo oggi è indubbiamente giunto da una fondamentale pronuncia del Tribunale federale costituzionale tedesco (Bundesverfassungsgericht, BVerfG), divenuta nota per essere stata la prima sentenza a fare riferimento al concetto di "autodeterminazione informativa" (informationelle Selbstbestimmung). Nel dicembre del 1983, il Tribunale pubblica una delle decisioni destinate a rimanere nella storia del nostro continente in occasione del sindacato di legittimità costituzionale di una legge federale riguardante il censimento dei cittadini tedeschi

[6] Il concetto di *informational privacy* è stato definito dallo statunitense Alan F. Westin come: "claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others", così WESTIN A., *Privacy and Freedom*, New York: Atheneum, 1967. È evidente dunque che in America, come in Europa, si avvertiva profondamente l'esigenza di ampliare la nozione di *privacy* nell'intento di tutelare l'individuo di fronte ai nuovi sistemi di sorveglianza. Sul punto si veda: DELLA MORTE G., *Big Data e Protezione Internazionale Dei Diritti Umani. Regole e Conflitti*, in ARCARI M., MILANO E., TANZI. A. (diretta da), *La ricerca del diritto nella comunità internazionale*, Editoriale scientifica, Napoli, 2018, pp. 141-142; HIJMANS H., *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU*, Law, Governance and Technology Series 31, Springer, 2016, pp. 39-40.

[7] FINOCCHIARO G., *Identità personale (diritto alla)*, in *Digesto delle discipline privatistiche, Sezione civile*, Torino, 2010, pp. 721 e ss.; DE HERT P., GUTWIRTH S., *Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action*, GUTWIRTH S., POULLET Y., DE HERT P., NOUWT J., DE TERWANGNE C. (eds), *Reinventing data protection?, ,* Springer, 2009, pp. 3 e ss.

(Volkszählungsgesetz).[8] La legge in questione, approvata l'anno precedente senza particolari obiezioni, aveva il dichiarato scopo di fungere da base normativa per l'esecuzione di un censimento volto ad avere cognizione della situazione socio-economica della popolazione, attraverso la raccolta, l'elaborazione e la successiva trasmissione ad altri enti amministrativi di dati attinenti a svariate dimensioni della vita quotidiana degli individui: dalla residenza agli spostamenti, dalla professione al credo religioso.[9] Il tribunale costituzionale, investito della questione grazie all'opposizione di quanti lamentavano un illegittimo eccesso della quantità di dati raccolti e la totale assenza di limiti con riguardo ad un loro successivo utilizzo, redige la sentenza che, nel dichiarare la parziale illegittimità costituzionale della legge, consente l'ingresso della autodeterminazione informativa fra le maglie dell'ordinamento costituzionale, piantando il seme da cui poi germoglieranno le teorie moderne in materia di trattamento di dati personali come diritto fondamentale. Per mezzo dell'esplicito richiamo al diritto alla personalità sancito dai primi due articoli della Costituzione federale, la Consulta spiega che uno dei corollari fondamentali di tale diritto generale si esplica necessariamente attraverso la possibilità di avere contezza di quali informazioni di carattere personale siano in circolazione e di poter intervenire nel momento in cui si dovessero concretizzare situazioni lesive della propria sfera giuridica.[10] Consci del ritardo del diritto rispetto alla tecnologia, i giudici dedicano particolare attenzione alle modalità di trattamento dei dati che stanno

[8] Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1983), 25.03.1982.
[9] SARTOR G., *Tutela della personalità e normativa per la «protezione dei dati». La sentenza della corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici del «Datenschutz»*, in *Informatica e Diritto*, 1986, pp. 95 e ss.
[10] BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83, par. 143-146.

repentinamente acquisendo capacità di controllo e di influenza senza precedenti. Ad avviso del Tribunale, in un'epoca in cui gli strumenti di analisi di dati sono in grado di comprimere indebitamente ed indirettamente lo sviluppo della personalità dell'individuo all'interno della collettività di appartenenza, giacché lo costringono a vivere in una situazione di inconsapevolezza e di involontaria esposizione che non gli permette di determinarsi liberamente, l'autodeterminazione informativa si manifesta quale presupposto fondamentale per assicurare il pieno godimento di diritti costituzionalmente garantiti.[11] Il passaggio appena evidenziato non consiste in una mera innovazione terminologica, ma rappresenta uno stravolgimento degli approdi giurisprudenziali precedenti: con la sentenza sulla legge sul censimento, l'autodeterminazione informativa smentisce la validità di quella "teoria delle sfere" (Sphärentheorie) che aveva guidato il BVerfG in tutti i suoi precedenti giudizi in materia di tutela dell'individuo nel contesto della raccolta delle sue informazioni personali. In base alla impostazione antecedente, il comportamento della persona può essere suddiviso in sfere concentriche in cui maggiore è l'intimità delle sue azioni, minore è l'ingerenza permessa ai soggetti esterni. Pertanto, sul piano normativo, le regole che consentono il trattamento delle informazioni attinenti alle attività che la persona svolge in ambiente pubblico e visibili allo sguardo altrui hanno un carattere dichiaratamente più permissivo rispetto a quelle che, per converso, sono rivolte a disciplinare il trattamento di dati riconducibili alla sfera privata. [12] Dunque, nell'intento di abbandonare un approccio che si è dimostrato inadeguato ai caratteri dell'elaborazione dei dati

[11] *Ibid*., parr. 143-146.
[12] SARTOR G., *Tutela della personalità e normativa per la «protezione dei dati»*, *op cit.*, pp. 100-107.

moderna, la sentenza supera la precedente impostazione multilivello che differenzia i dati personali a seconda dell'intensità del loro collegamento con l'interessato e procede ad un'operazione di uniformazione in ragione del fatto che i metodi di confronto incrociato di dati resi possibili dai sistemi più avanzati non permettono più di qualificare un'informazione come priva di significato o rilevanza.[13] Da tali premesse, la corte ricava un argomento solido in favore di una prospettiva diversa e, ad avviso di chi scrive, più consona ad una tutela effettiva. Non è più possibile limitarsi ad osservare il dato in sé per stabilire la legittimità dell'invasione nella sfera individuale, ma risulta, al contrario, imprescindibile una valutazione che prenda in considerazione anche il contesto in cui quel dato viene trattato (Verwendungszusammenhang).[14] Pertanto, già mezzo secolo fa il tribunale costituzionale aveva percepito le difficoltà che sarebbero derivate dalla questione definitoria in riferimento alla qualificazione dei dati e, contrariamente a quanto poi stabilito dalle fonti normative che hanno visto la luce nel corso degli anni successivi, si schiera apertamente in favore della tesi – sostenuta nell'ambito del presente lavoro – che definisce la natura del dato in dipendenza del contesto specifico di elaborazione, dunque delle risorse a disposizione del titolare del trattamento e delle finalità da questo perseguite.[15]

Ad ogni modo, nella definizione dei contorni di questo diritto, la corte esclude che esso possa assumere i connotati dell'assolutezza tipici dei regimi proprietari, atteso che la circolazione delle informazioni rappresenta un elemento indispensabile per una

[13] PALUMBO A., *Il diritto all'autodeterminazione informativa. L'esperienza tedesca in materia di protezione dei dati personali*, Tesi di dottorato, Università degli studi di Milano-Bicocca, 2015/16., pp. 73-74.
[14] BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83, par. 151.
[15] PALUMBO A., *Il diritto all'autodeterminazione informativa*, *op. cit.*, pp. 79-83.

collettività, il cui progresso è essenzialmente dipendente dalla comunicazione: "l'informazione, anche se concernente il singolo, è la rappresentazione di una realtà sociale, rappresentazione che non può essere esclusivamente assegnata a colui alla quale si riferisce".[16] Pertanto, sebbene l'autodeterminazione informativa conferisca alla persona fisica un potere dispositivo in relazione ai propri dati, tale diritto deve retrocedere quando la legge definisce come preminenti interessi di soggetti, pubblici o privati, diversi dall'interessato.[17] In merito alla questione di legittimità sollevata con riguardo alla legge sul censimento, la corte non fa altro che affermare in maniera chiara un principio dello Stato di diritto e impone che anche per il soddisfacimento dell'interesse pubblico alla mappatura della cittadinanza debba rinvenirsi una giustificazione giuridica in una legge che, oltre a consentire il trattamento, ne stabilisca i limiti.

Alla luce di tali osservazioni, la pronuncia del tribunale costituzionale tedesco è stata individuata quale prima tappa di questo viaggio in ragione del suo ruolo di pilastro nell'evoluzione del tema della protezione dei dati personali. La tensione che intercorre tra l'avanzamento della tecnologia e i principi dello Stato di diritto viene risolta avallando quell'approccio che vuole una disciplina "proattiva" atta a regolamentare qualsiasi tipo di trattamento senza, pertanto, caratterizzarsi come normativa repressiva intesa a punire solamente le ingerenze illegittime.[18] Da tale premessa derivano la previsione della necessità di una base giuridica per il trattamento, i principi di minimizzazione e finalità, il rilievo attribuito alla figura

[16] BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83, par. 148, nella traduzione offerta da G. SARTOR, *Tutela della personalità e normativa per la «protezione dei dati»*, op cit., p. 107.
[17] PALUMBO A., *Il diritto all'autodeterminazione informativa*, *op. cit.*
[18] SARTOR G., *Tutela della personalità e normativa per la «protezione dei dati»*, *op cit*., pp 112-114.

del responsabile per la protezione dei dati personali, elementi che oggi costituiscono parte integrante del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

In ogni caso, per quanto rileva ai fini della presente tesi, dalla lettura della sentenza è possibile evincere i motivi per cui il dato a carattere personale nasce – e rimane tuttora – il centro gravitazionale dell'impianto regolamentare europeo.[19] La notevole spinta in avanti generata dalla pronuncia della consulta tedesca, anche rispetto alle normative in materia introdotte in ambito continentale pochi anni prima, rappresenta la risposta decisa data dal potere giurisdizionale di fronte alla incipiente invasività dell'azione di un potere pubblico che sta inglobando nella macchina amministrativa le nuove tecnologie di elaborazione di informazioni, le quali, per mezzo del trattamento di dati personali di ogni tipo, nascondono concreti rischi di violazione di diritti costituzionalmente garantiti. Ciò vale, a maggior ragione, in un contesto in cui l'autorità motiva le sue ingerenze senza che vi sia una base normativa che renda legittime le sue pretese. Dunque, il Tribunale riesce nello scopo di aprire una nuova prospettiva sul tema, insistendo sul fatto che non è sufficiente assicurare una disciplina giuridica più severa nei soli confronti delle informazioni più intime poiché il nuovo strumentario a disposizione dei titolari del trattamento non permette più di accettare una distinzione tra informazioni comunque rientranti nella categoria del dato personale. Tuttavia, in questa fase ancora primordiale, il dibattito, tanto giurisprudenziale quanto dottrinale, continua a rimanere circoscritto alle informazioni relative alle persone fisiche.

[19] BRUGIOTTI E., *La privacy attraverso le "generazioni dei diritti". Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico*, in *dirittifondamentali.it*, 2/2013.

Come si tenterà di evidenziare nel corso di questo lavoro, nell'attuale epoca della *data analysis* e del *machine learning*, la massima stabilita dai giudici tedeschi potrebbe essere replicata in chiave estensiva in quanto, oramai, anche alcuni dati non personali sembrano non poter essere più considerati come irrilevanti.[20]

3. Il panorama internazionale in materia di protezione dei dati

Gli anni Ottanta hanno rappresentato un periodo florido per la progressiva specificazione della tutela dei dati a carattere personale come paradigma distinto rispetto alla *privacy*. Già pochi anni prima che la Corte costituzionale tedesca innescasse il dibattito con la sentenza di cui si è trattato in precedenza, due organizzazioni internazionali hanno permesso l'adozione di altrettanti atti espressamente dedicati alla regolamentazione del trattamento dei dati personali.

In riferimento a questi aspetti, è opportuno sin da subito sottolineare che, in ragione della vocazione collaborativa e pluralista delle organizzazioni internazionali, i principi da queste stabiliti non sono elaborati con esclusivo riguardo alla tutela dei diritti fondamentali delle persone fisiche, ma sono presenti anche disposizioni dedicate al sistema di trasferimento dei dati al di fuori dei confini di uno degli Stati parte. Ad ogni modo, l'oggetto della disciplina rimane il dato a carattere personale anche in questa circostanza, lasciando ancora una volta da parte le altre tipologie di dati che, specie nelle organizzazioni di stampo economico, rivestono un'importanza notevole.

[20] IRTI C., *Personal Data, Non-Personal Data, Anonymised Data, Pseudonymised Data, De-identified Data*, in SENIGAGLIA R., IRTI C., BERNES A. (eds.), *Privacy and Data Protection in Software Service*, Springer, 2022, p. 50.

In seno all'organizzazione per la cooperazione e lo sviluppo economico (OCSE), alle preoccupazioni inerenti ai rischi derivanti dal trattamento automatizzato di dati personali si aggiunsero quelle relative alle eventuali ripercussioni conseguenti all'entrata in vigore di normative relative alla protezione dei dati difformi fra i diversi Paesi membri dell'organizzazione, con particolare riferimento a quelle che introducevano obblighi di localizzazione dei dati, rallentando o impedendo la fondamentale circolazione transfrontaliera delle informazioni.[21]

Pertanto, le "*Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*", adottate nel 1980, mirano esattamente a prevenire il consolidamento degli effetti avversi della eterogeneità regolamentare attraverso l'introduzione di un insieme di principi basilari comuni a tutte le normative che disciplinano il trattamento di dati personali.[22] Le disposizioni riflettono in maniera evidente quegli interessi economici in cui risiede la ragion d'essere di questa organizzazione internazionale e che, nel caso di specie, hanno motivato un intervento volto ad impedire alle nascenti legislazioni nazionali in materia di ostacolare quel flusso di informazioni fra Paesi membri che aveva già dimostrato di essere vitale per il funzionamento e per lo sviluppo delle relazioni economiche transnazionali. Gli otto principi elencati vengono definiti come soglia minima a cui i singoli ordinamenti dei Membri avrebbero dovuto uniformarsi affinché il divieto di trasferimento transfrontaliero di informazioni non potesse essere giustificato sulla base della carente tutela dei diritti e delle libertà connessi al

[21] OECD, *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, op. cit.
[22] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 23 settembre 1980 - C(80)58/FINAL.

trattamento di dati nel luogo di destinazione.[23] La versione definitiva del testo rappresenta, difatti, il risultato di una complicata e delicata operazione di bilanciamento tra la tutela degli individui e la necessità di garantire la libera circolazione dei dati.

Tuttavia, degni di nota sono soprattutto i passaggi delle linee guida in cui vengono toccati aspetti che sono presentati come secondari rispetto ai principi e al nucleo del trattamento dei dati personali. Difatti, il documento dà prova di una certa consapevolezza anche in riferimento a ciò che si trova immediatamente al di fuori del mondo delle informazioni personali. È evidente che il trattamento di dati generalmente inteso è in grado di avere un notevole impatto, oltre che sulla protezione della *privacy* e delle libertà individuali, anche su altri settori che godono di propria rilevanza giuridica: le telecomunicazioni, il commercio, il diritto d'autore, ad esempio, comportano anch'essi raccolta, analisi e trasferimento di dati di varia natura e pertanto sono suscettibili di essere disciplinati da appositi strumenti normativi. Da tale premessa nasce la proposta, rimasta sulla carta, di estendere la disciplina sui dati personali anche ai dati relativi alle persone giuridiche o ai gruppi privi di personalità giuridica. I redattori del documento, nella spiegazione dei motivi per cui non si è formato un consenso sufficiente intorno a tale questione, fanno esplico riferimento alle difficoltà insite nell'operazione di distinzione tra dati di natura personale e dati non personali.[24]

[23] I principi sono quelli di *Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, Accountability*.

[24] Risulta di particolare interesse al riguardo il passaggio che recita: "Some countries consider that the protection required for data relating to individuals may be similar in nature to the protection required for data relating to business enterprises, associations and groups which may or may not possess legal personality. The experience of a number of countries also shows that it is difficult to define clearly the dividing line between personal and non- personal data. For example, data relating to a small company may also concern its owner or owners and provide personal information of a more or less sensitive nature. In such instances it may be advisable to extend to corporate entities the protection offered by rules relating primarily to

Ciononostante, la soluzione suggerita nella parte relativa ai commenti, secondo cui la linea di demarcazione dovrebbe essere rimessa alle normative dei singoli Stati membri, non convince affatto dal momento che, proprio alla luce della dimensione transnazionale della materia, demandare un compito così delicato alla volontà di differenti legislatori non farebbe altro che produrre ingenti problemi di eterogeneità normativa, contravvenendo, in sostanza, agli stessi obiettivi prefissati dalla OCSE.[25]

In ogni caso, malgrado l'autorevolezza delle *Guidelines*, l'assenza di vincolatività ne ha attenuato fortemente l'impatto, quantomeno in territorio europeo, dove contemporaneamente un'altra organizzazione internazionale stava lavorando ad un nuovo strumento atto a regolamentare l'elaborazione di dati personali. In seno al Consiglio d'Europa, il tema del trattamento delle informazioni per mezzo delle nuove tecnologie occupava già da qualche anno le agende dei membri del Comitato dei Ministri. Effettivamente, tale organo aveva adottato due risoluzioni in materia di tutela della riservatezza delle persone fisiche in rapporto alle banche dati elettroniche del settore privato e di quello pubblico già durante la prima metà degli anni Settanta.[26] Siffatti provvedimenti,

---

personal data", in OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, *op. cit.*

[25] Tale inciso risulta contraddittorio rispetto alla premessa delle *Guidelines*, specie nella parte in cui recitano: "For a number of reasons the problems of developing safeguards for the individual in respect of the handling of personal data cannot be solved exclusively at the national level. The tremendous increase in data flows across national borders and the creation of international data banks (collections of data intended for retrieval and other purposes) have highlighted the need for concerted national action and at the same time support arguments in favour of free flows of information which must often be balanced against requirements for data protection and for restrictions on their collection, processing and dissemination".

[26] Comitato dei Ministri del Consiglio d'Europa, Risoluzione (73) 22 sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore privato, del 26/09/1973; Comitato dei Ministri del Consiglio d'Europa, Risoluzione (74) 29 sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore pubblico, del 20/09/197.

benché difettassero di vincolatività, testimoniano, da un lato, una discreta preoccupazione avvertita nei confronti dell'emersione di nuovi strumenti di elaborazione dei dati e, dall'altro, una acquisizione di consapevolezza che l'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), relativo al rispetto della vita privata e familiare,[27] non fosse più ritenuto un baluardo abbastanza resistente, di per sé, a fronteggiare l'imperversare della tecnologia. Le risoluzioni in parola contengono, *in nuce*,[28] quei principi e quelle definizioni che verranno sviluppati ed inseriti, di lì a poco, nel primo strumento internazionale vincolante in materia: la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, n. 108 del 1981 (Convenzione n. 108).

Benché coeva alle *Guidelines* dell'OCSE e malgrado la collaborazione tra le due organizzazioni nella fase redazionale, sussistono poche ma significative differenze tra i due testi. Il carattere vincolante rende la Convenzione n. 108 uno strumento assai più incisivo rispetto ai principi stabiliti dall'OCSE e, come naturale conseguenza, comporta un maggiore livello di dettaglio nelle disposizioni, specie quelle di natura derogatoria. Altro aspetto differenziale degno di nota risiede nell'ambito di applicazione dei provvedimenti: mentre il Consiglio d'Europa ha preferito

[27] CEDU, art. 8 – Diritto al rispetto della vita privata e familiare: "1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui".

[28] Entrambe le Risoluzioni non riportano alcun riferimento al concetto di "identificabilità", in quanto recitano: "Ai fini della presente risoluzione, per "dato personale" si intende ogni informazione relativa a persone fisiche […]".

circoscrivere il perimetro normativo ai trattamenti automatizzati,[29] le *Guidelines* si contraddistinguono per un ambito applicativo definito in maniera meno rigida, in quanto destinate a quei dati personali che in ragione delle modalità, della natura e del contesto del trattamento, possono ingenerare un rischio di lesione alla privacy e alle libertà individuali.[30] Da tale configurazione deriva la scelta – che costituisce un ulteriore e rilevante punto di rottura rispetto alla Convenzione n. 108 – di non limitare il campo di applicazione del provvedimento ai soli trattamenti automatizzati, sulla scorta della constatazione, di ordine squisitamente pragmatico, secondo cui una decisione in senso contrario avrebbe inutilmente complicato un settore già di per sé gravido di difficoltà. Dunque, si avverte in maniera eclatante la presenza di due anime differenti all'interno dei rispettivi documenti poiché, malgrado l'identità della definizione di dato personale, da un lato, la Convenzione n. 108 adotta un approccio statico e predeterminato, in virtù del quale il dato e il tipo di trattamenti rientranti nella sua cornice normativa sono definiti *a priori*, con possibilità di interpretazioni estensive più limitata; dall'altro lato, l'OCSE sposa un'impostazione maggiormente dinamica e proiettata al rischio di pregiudizio per la persona fisica, variabile in dipendenza della situazione in cui le informazioni vengono trattate.

Dal punto di vista contenutistico, al di là dell'importanza dei principi riportati – liceità, finalità e adeguatezza – la Convenzione n.

[29] Art. 3, c. 1, Convenzione n. 108: "Le Parti si impegnano ad applicare la presente Convenzione alle collezioni automatizzate di dati a carattere personale e all'elaborazione automatica di tali dati nei settori pubblico e privato". Ad ogni modo, è doveroso sottolineare che la Convenzione stessa garantisce agli Stati membri la possibilità di allargare il campo di applicazione anche ai trattamenti non automatizzati, come recita l'art. 3, c. 2, lett. c): "[Qualsiasi Stato può comunicare] che esso applicherà la presente Convenzione anche alle collezioni di dati a carattere personale che non formano oggetto di elaborazione automatica".
[30] L'ambito di applicazione delle *Guidelines* dell'OCSE è così definito: "These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties".

108 assume particolare rilievo per il ruolo di supporto svolto con riguardo alla contestualizzazione giurisprudenziale della tutela dei dati personali. Sebbene i tempi non fossero ancora maturi per un distacco più accentuato dalla tutela della vita privata, la Corte di Strasburgo ha in più di un'occasione fatto ricorso a tale strumento per qualificare un trattamento di informazioni attinenti a persone fisiche come ingerenza indebita nella sfera privata degli individui, andando, per il suo tramite, a garantire il rispetto dell'art. 8 della CEDU.[31] Nell'ambito del Consiglio d'Europa, la scelta di attribuire una funzione complementare alla convenzione,[32] se, per un verso, è risultata obbligata in quanto non direttamente rientrante nell'alveo degli atti il cui rispetto è sottoposto al controllo della Corte di Strasburgo; per altro verso, ha comunque contribuito in maniera determinante all'avanzamento in direzione del definitivo riconoscimento del diritto alla protezione dei dati personali come fattispecie autonoma e fondamentale.

In chiusura dell'analisi della genesi internazionale del *data law*, rimane ferma l'ipotesi secondo cui la protezione non poteva che essere concepita primariamente come diritto riferito ai dati di natura personale. La caratterizzazione di tale tutela come costola del più

[31] Corte europea dei diritti umani, sentenze: Leander c. Svezia del 26 marzo 1987, Serie A n. 116; Kopp c. Svizzera del 25 marzo 1998, Repertorio 1998-II; Amann c. Svizzera (GC), n. 27798/95, 2000 - II.

[32] Invero, è opportuno osservare che la stessa Convenzione n. 108 evidenzia il ruolo ancillare e strumentale rispetto alla tutela della vita privata, sia nel preambolo, nella parte in cui recita "considerando che è auspicabile estendere la protezione dei diritti e delle libertà fondamentali di ciascuno, e in particolare il diritto al rispetto della vita privata, tenuto conto dell'intensificazione dei flussi internazionali di dati a carattere personale oggetto di elaborazione automatica" e ancora "riconoscendo la necessità di conciliare i valori fondamentali del rispetto della vita privata e della libera circolazione delle informazioni tra i popoli", sia nella definizione del suo oggetto all'articolo 1: "Scopo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano".

consolidato diritto al rispetto della vita privata, di cui ne è esempio la giurisprudenza della Corte europea dei diritti dell'uomo, ne ha irreversibilmente alterato il successivo processo di sviluppo, lasciando ben poco spazio ad interventi di tenore differente. È pur vero che il grado di avanzamento della tecnologia dell'epoca, che non poteva vantare l'odierna capacità di estrapolare significato da qualsiasi tipo di dato, non permetteva considerazioni di respiro più ampio e, per tali motivi, le informazioni di carattere non personale venivano, legittimamente, contemplate solo in qualità di elementi ancillari afferenti a specifiche normative di settore.

4. Il consolidamento della disciplina a livello comunitario: l'epoca delle direttive

Gli anni Novanta hanno inaugurato una stagione di importanti riforme per il vecchio continente in materia di disciplina dei dati. La corposa serie di interventi varati dal legislatore europeo che si sono succeduti in un arco di tempo piuttosto ristretto comincia con la Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, per l'appunto definita "Direttiva Madre".[33] Nonostante i risalenti moniti del Parlamento europeo,[34] la Direttiva in questione vede la luce solamente nel 1995,

[33] 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 (Gazzetta ufficiale n. L 281 del 23/11/1995).

[34] In particolare, si segnala la Risoluzione Parlamento europeo sulla tutela dei diritti dell'individuo di fronte al crescente progresso tecnico nel settore dell'informatica, approvata nella seduta di martedì 8 maggio 1979 (Doc. XII, n. 58), in cui, fra l'altro, viene rivolto un invito alla Commissione europea "a preparare una proposta di direttiva relativa all'armonizzazione delle legislazioni sulla tutela dei dati in modo da garantire una protezione al più alto livello per i cittadini della Comunità".

al termine di una non poco travagliata ricerca di una soluzione di compromesso fra le varie prospettive avanzate dagli Stati membri.[35]

Malgrado la Direttiva Madre costituisca un primo grande passo verso l'elaborazione di un diritto fondamentale alla protezione dei dati, [36] il provvedimento trae origine da considerazioni di carattere principalmente mercantilistico, come conferma la scelta di utilizzare l'articolo 100 A del Trattato istitutivo della Comunità europea come base giuridica.[37] Tale aspetto è imputabile a un duplice ordine di ragioni: da un lato, l'Unione europea non godeva ancora di una competenza specifica e autonoma in materia di trattamento di dati; dall'altro lato, la misura si prestava quale utile strumento per la realizzazione effettiva del mercato unico e per il relativo esercizio delle quattro libertà fondamentali riconosciute dai trattati istitutivi – la libera circolazione di persone, merci, servizi e capitali – il quale sarebbe stato indubbiamente ostacolato da normative di Stati membri eterogenee e concorrenti.[38]

Ciononostante, le norme non si esprimono secondo una logica squisitamente economica ma, al contrario, dimostrano piena consapevolezza della intima connessione che sussiste tra tutela dei

[35] FARO S., *Trattamento dei dati personali e tutela della persona*, in *Digesto delle Discipline* Pubblicistiche, appendice di aggiornamento, Torino, Utet, 2000, pp. 543-573.
[36] Proprio grazie a tale Direttiva, il diritto alla protezione dei dati personali otterrà finalmente riconoscimento normativo anche in Italia con la legge n. 675 del 31 dicembre 1996, necessaria ai fini dell'assolvimento degli obblighi di matrice comunitaria. Sul punto, si veda: SALERNO G. M., *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in NANIA R., RIDOLA P. (a cura di), *I diritti costituzionali*, vol. 2, Torino, 2006.
[37] La Direttiva 95/46/CE si fonda sull'articolo 100 A del Trattato istitutivo della Comunità europea, il quale attribuisce al Consiglio la competenza ad adottare misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno.
[38] Eloquente a tal proposito è il considerando n. 3 della Direttiva 95/46/CE: "considerando che l'instaurazione e il funzionamento del mercato interno, nel quale, conformemente all'articolo 7 A del trattato, è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali, esigono non solo che i dati personali possano circolare liberamente da uno Stato membro all'altro, ma che siano altresì salvaguardati i diritti fondamentali della persona".

dati personali e diritti fondamentali,[39] probabilmente anche per merito dell'articolo 8 della CEDU e della Convenzione n. 108 del Consiglio d'Europa, modelli a cui il testo si è dichiaratamente ispirato.[40] Dunque, la Direttiva nasce come provvedimento di matrice economica, ma, sotto il profilo del contenuto sostanziale delle norme, va al di là della stretta base giuridica che ne ha consentito l'adozione, spingendosi nel limitrofo ambito della protezione dell'individuo in quanto tale.[41]

In questo senso, gli articoli della Direttiva Madre costituiscono un primo tratteggio di quel carattere europeo della disciplina dei dati personali. Difatti, sono presenti alcuni profili di particolare rilievo che rimarranno dei capisaldi nel corso dell'evoluzione giuridica della disciplina: l'ambito di applicazione esteso ai trattamenti non automatizzati,[42] il rispetto degli obblighi imposto a soggetti che vantano un collegamento con il territorio dell'Unione senza esservi direttamente stabiliti,[43] l'istituzione di una autorità di controllo indipendente con il compito di monitorare l'osservanza delle regole [44] e, infine, una disciplina in materia di trasferimento dei dati verso Paesi extracomunitari che si traduce, come si vedrà meglio in seguito, in un obbligo di localizzazione.[45]

---

[39] Art. 1, comma 1, Direttiva 95/46/CE: "Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali".

[40] Direttiva 95/46/CE, cons. nn. 10 e 11. Quest'ultimo, in particolare, recita "considerando che i principi della tutela dei diritti e delle libertà delle persone, in particolare del rispetto della vita privata, contenuti dalla presente direttiva precisano ed ampliano quelli enunciati dalla convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone con riferimento al trattamento automatizzato dei dati di carattere personale".

[41] FARO S., *Trattamento dei dati personali e tutela della persona, op. cit.*

[42] Art. 3, comma 1, Direttiva 95/46/CE.

[43] Art. 4, comma 1, *lett.* c), Direttiva 95/46/CE.

[44] Art. 28, Direttiva 95/46/CE.

[45] Artt. 25 e 26, Direttiva 95/46/CE.

Per quanto attiene alla definizione di dato personale, la Direttiva propone una adeguata risposta alle preoccupazioni che, al tempo, iniziava a suscitare lo sviluppo della tecnologia, specie la diffusione di internet che, dopo anni come appannaggio delle istituzioni pubbliche, cominciava ad entrare nelle case dei cittadini comuni. Pertanto, l'articolo 2, lettera a) della Direttiva contiene una definizione estensiva di dato personale e, in particolare, aggiunge delle utili specificazioni,[46] con l'intento di ricomprendere nel proprio alveo svariate tipologie di informazioni che solo latamente potevano qualificarsi come personali.[47]

Con riguardo al tipo di strumento prescelto dal legislatore europeo nel 1995, la direttiva non può spingersi oltre la statuizione di principi generali volti ad innalzare il livello di armonizzazione, i quali, in ogni caso, necessitano di attuazione e di specificazione da parte degli Stati membri destinatari. La discrezionalità garantita dalla Direttiva ha avuto due conseguenze importanti sul piano della produzione normativa immediatamente successiva.

In primo luogo, l'abuso del margine di apprezzamento garantito ai singoli Stati membri ha determinato il mancato raggiungimento dell'anelato obiettivo di armonizzazione normativa fra le legislazioni nazionali. Sebbene la Corte di giustizia avesse a più riprese ricordato che la Direttiva Madre non mirava ad una armonizzazione "minima" ma, in linea di principio completa,[48] la fase di attuazione si è tradotta in un incremento delle differenze fra le discipline dei Paesi europei, con tutto quanto ne consegue nei

[46] Art. 2, *lett*. a), Direttiva 95/46/CE.
[47] BERNAL P., *Internet Privacy Rights Rights to Protect Autonomy*, in *Cambridge Intellectual Property and Information Law*, *Cambridge University Press*, 2014, pp. 87-97.
[48] Corte di Giustizia, 6-11-2003, causa C-101/01, Lindqvist; Corte di Giustizia, 24-11-2011, Cause riunite C-468/10 e C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) contro Administración del Estado.

confronti della libera circolazione infra-comunitaria dei dati personali. Sulla scorta, fra l'altro, di queste considerazioni avrà origine qualche anno dopo la volontà di cambiamento delle istituzioni europee che, nel contesto del necessario aggiornamento di una normativa vetusta, opteranno per uno strumento con un effetto di uniformazione ben più elevato, il regolamento.[49]

In secondo luogo, il grado di astrattezza dei principi sanciti nella Direttiva mal si conciliava con la necessità di regolamentazione di settori particolari dell'economia europea, contraddistinti da una forte vocazione transnazionale, dove il trasferimento delle informazioni non costituiva un elemento ancillare ma il cuore dell'attività stessa. Pertanto, la necessità di intervenire attraverso discipline di settore più specifiche e più concrete rispetto a quanto già previsto dalla Direttiva Madre – la quale rimaneva comunque applicabile quando non espressamente derogata – ha dato il via ad una ulteriore stagione di interventi normativi riguardanti il trattamento dei dati.[50]

La prima fra le misure emanate allo scopo di declinare sul piano concreto i principi della Direttiva Madre è stata la Direttiva 97/66/CE relativa al settore delle telecomunicazioni,[51] dove trovano spazio i medesimi obiettivi di tutela della vita privata e di libera circolazione delle informazioni. Una particolarità della normativa risiede, invece, nel richiamo esplicito ai legittimi interessi delle persone giuridiche, la cui tutela diventa un obiettivo aggiunto della

[49] VOIGT P., VON DEM BUSSCHE A., *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, 2017, pp. 1-3.
[50] CORTESE B., *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona,* in *Il Diritto dell'Unione europea*, n. 2 del 2013, pp. 313 e ss.
[51] 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 (Gazzetta ufficiale n. L 024 del 30/01/1998).

direttiva.[52] Dunque, in un settore particolarmente delicato anche per le persone giuridiche vengono incluse nel novero delle informazioni degne di tutela anche quelle non riconducibili ad individui identificati o identificabili. Malgrado la netta – e opportuna – demarcazione tra i diritti e libertà delle persone fisiche, da un lato, e i legittimi interessi di quelle giuridiche, dall'altro,[53] il legislatore europeo dimostra in questa direttiva un primo, benché timido, coinvolgimento di dati diversi da quelli personali.[54]

Sulla stessa linea si colloca la successiva Direttiva 2002/58/CE volta, per l'appunto,[55] ad adeguare la normativa del 1997 al progresso che nel frattempo ha investito la società dell'informazione in maniera tale da assicurare un livello di armonizzazione consono anche con riguardo ai nuovi servizi di comunicazione elettronica.[56] Il nuovo articolato predispone una serie di obblighi in capo agli operatori del settore delle comunicazioni elettroniche, fra i quali figurano quelli di assicurare la sicurezza dei

[52] Art. 1, comma 2, Direttiva 97/66/CE.
[53] La differenza tra persone fisiche e giuridiche concerne anche le prerogative ad esse attribuite. Un esempio di ciò è presente nel considerando n. 21, quando afferma: "considerando […] che il diritto al rispetto della vita privata delle persone fisiche e i legittimi interessi delle persone giuridiche richiedono che gli abbonati possono determinare in quale misura i loro dati personali debbano essere pubblicati nei medesimi elenchi; che gli Stati membri possono riconoscere questa possibilità ai soli abbonati che sono persone fisiche".
[54] A tale proposito, la Direttiva 97/66/CE esclude qualsiasi automatismo della estensione di tutela alle persone giuridiche nel considerando n. 13, dove afferma: "considerando che gli abbonati di un servizio di telecomunicazione offerto al pubblico possono essere persone fisiche o giuridiche; che le disposizioni della presente direttiva sono volte a tutelare, integrando la direttiva 95/46/CE, i diritti fondamentali delle persone fisiche, in particolare il loro diritto alla vita privata, nonché i legittimi interessi delle persone giuridiche; che tali disposizioni non possono in alcun caso comportare per gli Stati membri l'obbligo di estendere l'applicazione della direttiva 95/46/CE alla tutela dei legittimi interessi delle persone giuridiche; che questa tutela è assicurata nel quadro della normativa comunitaria e nazionale applicabile".
[55] Direttiva 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 (Gazzetta ufficiale n. L 201 del 31/07/2002).
[56] Direttiva 2002/58/CE., cons. nn. 4 e 5.

servizi oppure di cancellare o anonimizzare i dati di traffico,[57] e introduce un sistema di *opt-in* per le comunicazioni commerciali effettuate tramite sistemi automatizzati.[58] In merito al tipo di dati rientranti nel suo campo di applicazione, la Direttiva 2002/58/CE riprende, come detto, l'impostazione della normativa che sostituisce, ricomprendendo anche i "legittimi interessi degli abbonati che sono persone giuridiche",[59] e, invero, sembra spostare ulteriormente l'orizzonte quando, nella definizione delle categorie di "dati relativi al traffico" e "dati relativi all'ubicazione" viene preso in considerazione qualsiasi dato, senza che sia accompagnato dalla specificazione relativa al carattere personale dello stesso.[60] Cionondimeno, un'interpretazione che facendo leva sul combinato disposto di questi passaggi volesse intravedere una sorta di tutela generalizzata anche per i dati a carattere non personale rischia di essere prontamente smentita dal fatto che la Direttiva in discussione rimane pur sempre una declinazione in chiave settoriale della Direttiva Madre la quale, con le sue definizioni applicabili salvo disposizione contraria,[61] mantiene ben saldo il legame con i dati a carattere personale.

In seguito, il legislatore continentale ha continuato il suo percorso di specificazione della disciplina in materia di dati, ma sempre rimanendo all'interno dell'alveo delle informazioni personali. A tale proposito, appartiene allo stesso filone di sviluppo normativo la successiva Direttiva 2006/24/CE che aggiorna la precedente del 2002, ma che, al contempo, è incentrata sugli obblighi di conservazione dei dati in capo ai fornitori di servizi di

[57] Artt. 4 e 6, Direttiva 2002/58/CE.
[58] Art. 13, Direttiva 2002/58/CE.
[59] Art. 1, comma 2, Direttiva 2002/58/CE.
[60] Art. 2, *lett*. b) e c), Direttiva 2002/58/CE.
[61] Art. 2, prima parte, Direttiva 2002/58/CE.

comunicazione elettronica ai fini di indagine, accertamento e perseguimento di reati gravi.[62] Di nuovo, i dati relativi al traffico ed alla ubicazione disciplinati dalla direttiva possono riguardare le persone giuridiche,[63] ma pur sempre nel ben definito contesto della Direttiva 95/46/CE, della quale costituisce una diramazione. Tuttavia, più che per le innovazioni apportate alla disciplina previgente, l'atto in questione viene ricordato per la travagliata storia giuridica che lo ha caratterizzato, culminata con la sua invalidazione ad opera della Corte di giustizia dell'Unione europea con la celebre sentenza "*Digital Rights Ireland*".[64] Ad avviso della Corte, il legislatore europeo non aveva individuato il giusto equilibrio tra la tutela dei dati personali e la sicurezza pubblica: gli obblighi di conservazione imposti dalla direttiva non erano considerati proporzionati rispetto ai diritti legati alla riservatezza e alla protezione dei dati personali.[65]

Prima di concludere l'analisi dei provvedimenti del diritto primario europeo che hanno scandito questa stagione, è opportuno menzionare una ulteriore direttiva che, a differenza di tutte quelle analizzate in precedenza, sposta per la prima volta l'attenzione verso una tutela specificamente dedicata ai dati in qualità di bene giuridico

[62] 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 (Gazzetta ufficiale dell'Unione europea, L 105, 13/04/2006).
[63] Art. 1, comma 2, Direttiva 2006/24/CE.
[64] Corte di Giustizia, 8-4-2014, cause riunite C-293/12 e C-594/12, Digital Rights Ireland Ltd.
[65] 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 *Dpce online*, 2/2017, 349 ss.; TRUCCO L., "*Data retention": la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giurisprudenza italiana*, 2014, 1850 ss.

autonomamente considerato,[66] ossia come fine proprio e non in quanto mezzo strumentale alla protezione e all'esercizio di altri diritti.[67] La Direttiva 96/9/CE relativa alla tutela giuridica delle banche di dati, entrata in vigore allo scopo di assicurare garanzie adeguate ed uniformi per i "costitutori" di *database*,[68] introduce due diversi strumenti di tutela. Il primo concerne le banche dati frutto della creazione dell'ingegno, le quali sono protette per mezzo del riconoscimento di una peculiare fattispecie di diritto d'autore;[69] il secondo, si traduce in un diritto espressamente definito "*sui generis*" che mira a proteggere le banche dati "non originali" la cui costituzione non è stata ottenuta per mezzo di un'attività creativa, ma grazie ad un investimento rilevante sotto il profilo qualitativo e quantitativo.[70]

Per quanto concerne l'oggetto, la Direttiva del 1996 non mira a tutelare il singolo dato che compone l'insieme ma, in un'ottica di incentivazione nella creazione di *database*, delimita il suo ambito di applicazione alle raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti.[71] In sostanza, il diritto *sui generis*, vera e propria innovazione di questa normativa, permette l'utilizzo di parti circoscritte e, naturalmente, di singoli dati senza che sia necessaria l'autorizzazione del costitutore, giacché limita l'area di tutela a quelle parti della banca di dati che vengono definite

[66] Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati (Gazzetta ufficiale n. L 077 del 27/03/1996).
[67] In tal senso, sempre a cavallo tra gli anni Novanta e i primi anni Duemila, erano state emanate altre direttive che, toccando il tema dei dati in maniera tangenziale, erano destinate a disciplinare altri ambiti normativi della società dell'informazione, dove i dati stessi ricoprivano un ruolo strumentale. Fra queste, si ricordano la Direttiva 2000/31/CE sul commercio elettronico e la Direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione.
[68] Direttiva 96/9/CE, considerando n. 48.
[69] Cap. II, Direttiva 96/9/CE.
[70] Cap. III, Direttiva 96/9/CE.
[71] Art. 1, comma 2, Direttiva 96/9/CE.

come "sostanziali". [72] Ad ogni modo, malgrado l'ambito di applicazione della normativa risulti piuttosto modesto, questa direttiva rappresenta un passaggio importante nella storia dell'ordinamento europeo, sia per le interessanti, benché ridotte nel numero, decisioni della Corte di giustizia dell'Unione europea,[73] sia perché da essa sono scaturiti i primi dibattiti in merito alla regolamentazione della proprietà e dell'accesso ai dati. [74] Quest'ultimo aspetto in particolare, ritornato in voga negli ultimi anni dopo che la diffusione dei *Big Data* ha palesato una possibile inadeguatezza della Direttiva 96/9/CE di fronte alle nuove sfide poste dalla attuale economia dei dati, verrà approfondito nel capitolo terzo, quando si esaminerà il tema della *data ownership*.

Nel complesso, questa fase della produzione normativa continentale restituisce un ordinamento dettagliato e, al contempo, variegato, dove il legislatore ha dato prova di una spiccata sensibilità

[72] La direttiva non indica una porzione esatta affinché la parte possa essere considerata sostanziale. Difatti, alcune divergenze nell'interpretazione giuridica di tale nozione sono giunte dalle pronunce della giurisprudenza degli Stati membri. A tale riguardo, si veda: Commission Staff working document, *Evaluation of Directive 96/9/EC on the legal protection of databases* (SWD (2018) 147 final), pp. 28 e *ss*.

[73] Corte di Giustizia, 9-11-2004, causa C-338/02, Fixtures Marketing Ltd *c*. Svenska Spel AB; Corte di Giustizia, 9-11-2004, causa C-444/02, Fixtures Marketing Ltd *c*. Organismos prognostikon agonon podosfairou AE (OPAP); Corte di Giustizia, 9-11-2004, causa C-46/02, Fixtures Marketing Ltd c. Oy Veikkaus Ab; Corte di Giustizia, 9-11-2004, causa C-203/02, The British Horseracing Board Ltd *c*. William Hill Organization Ltd. Per mezzo di queste decisioni, la Corte fornisce una interpretazione piuttosto restrittiva del diritto *sui generis*, distinguendo tra la "creazione" dei dati – non coperta dalla Direttiva 96/9/CE – ed il loro "ottenimento", che, invece, ricade nell'ambito di applicazione della direttiva. Così opinando, la Corte sembra abbracciare la cosiddetta "*spin-off doctrine*", ossia la tesi sulla scorta della quale il diritto in questione viene riconosciuto solo per gli investimenti direttamente attribuibili al conseguimento, alla verifica ed alla presentazione della banca dati, sulla base di una logica di incentivazione della generazione dei database ed escludendo, conseguentemente, la protezione per le raccolte di dati generate quasi "automaticamente" come *by-product* di un'altra attività. Sul punto, si veda: DAVISON M. J., HUGENHOLTZ, P. B., *Football fixtures, horseraces and spin offs: the ECJ domesticates the database right*, in *European Intellectual Property Review*, n. 3, 2005.

[74] LEISTNER M., *Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform*, in LOHSSE S., SCHULZE R., STAUDENMAYER D. (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools*, 2017.

in riferimento al tema dei dati. In particolare, malgrado la Direttiva da ultimo analizzata costituisca un *novum* rilevante nel contesto internazionale, l'attenzione è stata inevitabilmente catturata dai dati a carattere personale. Tuttavia, è possibile intravedere già dagli albori dello sviluppo della disciplina europea dei dati quella tensione tra lo spirito mercantilistico, testimoniato dalle basi giuridiche sulle quali si fondano tutte le direttive in commento, e la vocazione, sviluppatasi sul finire degli anni Novanta, di organizzazione internazionale interessata anche ai diritti fondamentali, elemento che condurrà, di lì a poco, ad un cambiamento radicale nella concezione della tutela dei dati personali.

5. La costituzionalizzazione del diritto alla protezione dei dati personali: dalla Carta europea dei diritti fondamentali al riconoscimento da parte della Corte di giustizia dell'Unione europea

Le istanze dottrinali favorevoli ad una maggiore autonomia del diritto alla protezione dei dati personali trovano finalmente riscontro a livello (para)normativo con l'inizio del XXI secolo. La Carta dei diritti fondamentali dell'Unione europea (la Carta), proclamata a Nizza nel dicembre del 2000, riportando il diritto al rispetto della vita privata della vita familiare all'articolo 7 e la protezione dei dati di carattere personale nell'articolo 8, costituisce il primo atto della storia giuridica europea a disciplinare distintamente due situazioni giuridiche soggettive da sempre concepite come parti di un unico corpo. La rilevanza indiscussa di tale episodio è stata inizialmente limitata dall'assenza di valore vincolante della Carta di Nizza: il documento era stato redatto con lo scopo di avere un riscontro testuale per le istituzioni comunitarie in tema di diritti a carattere fondamentale, il riferimento ai quali si rinveniva per lo più solo nelle

sentenze della Corte di giustizia. Pertanto, la Carta si presenta come elaborazione di natura ricognitiva dei diritti fondamentali emergenti dalle tradizioni costituzionali degli Stati membri dell'Unione, ma senza che ancora potesse fungere da base normativa autentica per l'esercizio dei diritti in essa sanciti.[75]

L'ulteriore strato di tutela che viene predisposto dalla Carta rappresenta il frutto più evidente di quel percorso di progressivo affrancamento volutamente perseguito dal legislatore europeo che, accanto alla libertà di stampo negativo correlata alla riservatezza così come originata in terreno statunitense, aggiunge *expressis verbis* l'ulteriore dimensione positiva, quella dell'autodeterminazione informativa teorizzata dal tribunale costituzionale tedesco nel 1983, dirigendosi in tal guisa verso una effettiva costituzionalizzazione del diritto alla protezione dei dati personali.[76]

Il raggiungimento di un approdo di simile portata si colloca al culmine di un processo di gestazione che ha visto le corti sovranazionali ricoprire la parte di indiscusse protagoniste. Tanto la Corte europea dei diritti dell'uomo quanto la Corte di giustizia dell'Unione europea hanno condotto, nell'epoca antecedente alla proclamazione della Carta, un'indefessa opera di riconoscimento del diritto alla protezione dei dati personali, quale componente indefettibile del già positivizzato diritto alla protezione della vita privata e familiare. In primo luogo, è la Corte di Strasburgo a dare forma e contenuto al diritto in esame in occasione di pronunce riguardanti vicende concernenti temi differenti, ma tutti accomunati

[75] BIFULCO R., CARTABIA M., CELOTTO A., *Introduzione*, in BIFULCO R., CARTABIA M., CELOTTO A., L'Europa dei diritti, Bologna, 2001, pp. 12 e ss.
[76] POLLICINO O., BASSINI M., *Commento all'art. 8 CdfUE*, in *Carta dei diritti fondamentali dell'Unione europea*, MASTROIANNI R., POLLICINO O., ALLEGREZZA S., PAPPALARDO F., RAZZOLINI O. (a cura di), Milano, 2017, pp. 132 e ss.; ALLEGRI M. R., *Ubi Social, Ibi Ius. Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei provider*, Milano, Franco Angeli, 2018, pp. 75-80.

dalle potenziali lesioni che la sfera giuridica dell'individuo avrebbe potuto subire a seguito del trattamento di informazioni che lo riguardavano.[77] Come confermato dalle sentenze più recenti,[78] la maggiore attenzione prestata alla tutela dei dati personali è andata di pari passo con lo sviluppo e la diffusione delle tecnologie dell'informazione che hanno accentuato l'esigenza di guarentigie più efficaci, in ragione dell'incremento del potere di ingerenza consentito dalla strumentazione moderna. A tale riguardo, non va dimenticato il ruolo ricoperto dalla Convenzione del Consiglio d'Europa n. 108 del 1981: malgrado, come detto, non fosse uno strumento di diritto internazionale direttamente giustiziabile dalla Corte europea, la risonanza avuta dalla Convenzione ha facilitato l'operazione di graduale riconoscimento del diritto alla tutela dei dati personali in seno alle norme applicabili agli Stati parte del Consiglio d'Europa.

Forte di un supporto normativo ben più solido, segnatamente la Direttiva 95/46/CE, la Corte di giustizia dell'Unione europea ha continuato l'attività di modellamento della nascente tutela dei dati personali sulla scia di quanto fatto dalla Corte di Strasburgo. Sin dalle decisioni più risalenti nel tempo,[79] il filo rosso che collega le sentenze dei giudici comunitari risiede nella spiccata vocazione al superamento della originaria caratterizzazione della protezione della riservatezza e dei dati personali come eccezioni alle libertà economiche sancite dai Trattati istitutivi, e nella conseguente volontà di fornire una lettura autenticamente finalizzata alla tutela di diritti

[77] Per una approfondita disamina dell'evoluzione giurisprudenziale, si veda *ibid*.
[78] Corte europea dei diritti dell'uomo, Editorial Board of Pravoye Delo and Shtekel *c.* Ucraina (ric. 33014/05), 5/5/2011.
[79] Corte di Giustizia, 12/11/1969, causa C-29/69, Stauder.

fondamentali, in una prospettiva, per l'appunto, costituzionale.[80] Del resto, i giudici comunitari si sono sempre mossi con l'obiettivo di dotare, in via interpretativa, l'impianto europeo di quei diritti fondamentali che i trattati istitutivi non contemplavano in ragione della missione essenzialmente economica perseguita dalla Comunità europea.[81] Nel contesto di tale opera di estrapolazione dei diritti fondamentali, dove la Corte di giustizia ha dichiaratamente attinto tanto dalle "tradizioni costituzionali comuni agli Stati membri" quanto dagli "strumenti internazionali concernenti la tutela dei diritti dell'uomo, cui gli stati membri hanno collaborato o aderito",[82] ha trovato spazio anche il diritto alla protezione dei dati personali, di riflesso alla tutela della riservatezza, per merito altresì dei richiami alla giurisprudenza della Corte europea dei diritti dell'uomo.

L'ampliamento degli interessi della Comunità europea, che da organizzazione per la regolazione dei rapporti economici si stava trasformando anche in unione di stampo politico, imponeva la positivizzazione di principi che, benché di importanza capitale, rimanevano ancora di natura pretoria. Questi fondamentalmente sono stati i presupposti che hanno stimolato la redazione della Carta dei diritti fondamentali, la quale, è bene ricordare, non godeva ancora di valore vincolante al momento della sua proclamazione nel 2000.

In ogni caso, per quanto qui di interesse, alla Carta va riconosciuto parimenti il merito di aver portato a termine l'*iter* avviato il secolo precedente, codificando separatamente il diritto alla

[80] ROSSI DAL POZZO F., *La giurisprudenza della Corte di giustizia sul trattamento dei dati personali*, in *Associazione Italiana Studiosi di Diritto dell'Unione europea* (AISDUE), *Sezione "Convegni annuali e interinali"*, n. 9, 2019, pp. 127 e ss.
[81] GALETTA D.U., *La tutela dei diritti fondamentali (in generale, e dei diritti sociali in particolare) nel diritto UE dopo l'entrata in vigore del Trattato di Lisbona*, in *Rivista italiana di diritto pubblico comunitario*, Anno XXIII, Fasc. 5-6, 2013, pp. 1175 e ss.
[82] Corte di Giustizia, 13/12/1979, causa C-44/79, Liselotte Hauer *c.* Land Rheinland-Pfalz.

riservatezza e quello alla protezione dei dati personali.[83] Nel tentativo di delineare con maggiore precisione la distinzione rispetto al diritto al rispetto della vita privata sancito dall'articolo 7,[84] l'articolo 8 non si arresta ad una mera affermazione di principio, ma definisce in maniera puntuale gli elementi che compongono lo scudo giuridico a tutela delle informazioni personali. I commi secondo e terzo fanno tesoro degli insegnamenti della giurisprudenza – anche di Strasburgo –[85] e del diritto derivato e incorporano i principi di lealtà, finalità e legalità, i diritti di accesso e rettifica e, da ultimo, la necessità di controllo di un'autorità indipendente.[86] La formulazione di dettaglio approvata dagli organismi europei permette di svolgere alcune riflessioni in merito alla carica avveniristica delle disposizioni ivi inserite. Il carattere innovativo dell'articolo non va rintracciato tanto nella sua qualificazione di "diritto di diversa origine", ossia non direttamente derivante dalla Convenzione europea o dalle tradizioni costituzionali dei Membri, quanto piuttosto nella discrezionalità esercitata dai redattori della Carta nell'attribuire a questa protezione la veste di diritto fondamentale.[87] È in questo senso, dunque, che la Carta può considerarsi destituita dell'accezione

[83] RODOTÀ S., *Data Protection as a Fundamental Right*, in GUTWIRTH S., POULLET Y., DE HERT P., DE TERWANGNE C., NOUWT S. (eds), *Reinventing Data Protection?*, Springer,2009, pp. 77 e ss.

[84] L'art. 7 della Carta dei diritti fondamentali dell'Unione europea recita: "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni".

[85] PARISI N., *Funzione e ruolo della Carta dei diritti fondamentali nel sistema delle fonti alla luce del Trattato di Lisbona*, in *Il diritto dell'Unione europea*, a. XIV, fasc. 3, 2009, pp. 663-664.

[86] Per la sua rilevanza, si ritiene opportuno riportare integralmente il testo dell'art. 8 – Protezione dei dati di carattere personale: "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".

[87] ADAM R., *Da Colonia a Nizza: la Carta dei diritti fondamentali dell'Unione europea*, in *Il Diritto dell'Unione Europea*, n. 4/2000, pp. 887-888.

di documento a carattere meramente ricognitivo dell'esistente: non perché con la codificazione dell'articolo 8 viene creato un diritto *ex novo*, ma in quanto viene riconosciuto a tale diritto, già presente nella trama ordinamentale europea,[88] un valore che prima non aveva.

Malgrado il risultato particolarmente significativo raggiunto con la Carta di Nizza, nella fase transitoria immediatamente successiva alla sua proclamazione, ma antecedente alla acquisizione di vincolatività, nelle prime pronunce giurisprudenziali non compaiono riferimenti concreti né al documento, né ai principi in esso sanciti.[89] La Corte rimane ancorata alla precedente impostazione secondo la quale alla tutela dei dati personali competeva la qualifica di eccezione alla regola generale del libero esercizio dell'attività economica.[90]

In prossimità dell'entrata in vigore del Trattato di Lisbona, firmato il 13 dicembre 2007, e della conseguente attribuzione di efficacia vincolante alla Carta dei diritti fondamentali, si percepisce un preliminare cambio di rotta da parte dei giudici di Lussemburgo.[91] Nella metaforica competizione tra libertà economiche, da un lato, e tutela dei dati personali come diritto fondamentale dall'altro, la sentenza *Promusicae* segna un considerevole ravvicinamento della seconda rispetto alle prime.[92] Nel contesto di una vicenda in cui il rinvio pregiudiziale sollevava un interrogativo in merito alla sussistenza di un'imposizione per gli Stati membri di istituire un

[88] Oltre a quanto disposto dal diritto derivato, dal diritto degli Stati membri e dalla giurisprudenza di Lussemburgo e di Strasburgo, il diritto alla protezione delle persone fisiche con riguardo al trattamento dei dati personali era già sancito dall'art. 286 del Trattato istitutivo della Comunità europea, con specifico riguardo ai trattamenti effettuati dalle istituzioni e dagli organismi comunitari.
[89] Corte di Giustizia, 6-11-2003, causa C-101/01, Lindqvist.
[90] POLLICINO O., BASSINI M., *Commento all'art. 8 CdfUE*, *op. cit.*, p. 141.
[91] CALZOLAIO S., *Protezione dei dati personali*, in BIFULCO R., CELOTTO A., OLIVETTI M., (a cura di), *Digesto delle Discipline Pubblicistiche*, Utet giuridica, 2017, pp. 620-624.
[92] Corte di Giustizia, 29-1-2008, causa C-275/06, Promusicae.

obbligo di comunicazione di dati personali per i fornitori di accesso alla rete o di servizi di archiviazione allo scopo di tutelare il diritto d'autore, i costanti riferimenti alla Carta di Nizza rendono evidente che le sue disposizioni hanno ormai fatto breccia nel *reasoning* della Corte di giustizia, malgrado non (ancora) direttamente applicabili.[93] Nel fornire la propria soluzione interpretativa, i giudici compiono un passo in avanti importante nella parte in cui, accennando all'articolo 8 della Carta, rimarcano la sua "genuinità" rispetto all'articolo 7 della Carta medesima e dunque, di riflesso, rispetto anche all'articolo 8 della CEDU.[94]

Tale spinta verso la costituzionalizzazione impressa dalla giurisprudenza è stata accolta non molto tempo dopo dal legislatore continentale con il Trattato di Lisbona, entrato in vigore il 1° dicembre 2009, per il tramite di due disposizioni di rilevanza epocale.

In primo luogo, la previsione dell'articolo 6 del TUE riconosce definitivamente alla Carta dei diritti fondamentali dell'Unione europea lo stesso valore giuridico dei Trattati istitutivi. A tale proposito, occorre mettere in evidenza che la norma non si limita semplicemente ad attribuire alla Carta efficacia vincolante, ma arriva ad equipararla alle fonti di diritto primario dell'Unione, garantendogli in tal modo il carattere di supremazia gerarchica tipico dei testi di rango costituzionale. In un certo senso, l'articolo 6 positivizza in un testo normativo la definitiva trasformazione

[93] Oltre agli ovvi richiami alle fonti di diritto derivato rilevanti nel caso di specie, i riferimenti alle disposizioni della Carta non si limitano agli articoli 7 e 8, ma comprendono anche l'art. 17 relativo al diritto di proprietà e l'art. 47 concernente il diritto a un ricorso effettivo ed a un giudice imparziale.

[94] A tale proposito, merita di essere riportata parte del paragrafo 64 della sentenza: "L'art. 7 [della Carta] riproduce in sostanza l'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950, il quale garantisce il diritto al rispetto della vita privata, mentre l'art. 8 della Carta proclama espressamente il diritto alla tutela dei dati personali".

dell'Unione europea da organizzazione di carattere prettamente mercantilistico a "spazio di libertà, sicurezza e giustizia",[95] dove il rispetto dei diritti individuali viene assicurato in modo diffuso e paritario, a prescindere dalla loro genesi e dal loro ambito di interesse.[96]

Le implicazioni giuridiche scaturite dall'inserimento dell'articolo 6 del TUE nel tessuto ordinamentale europeo non si sono arrestate al significato letterale delle parole in esso riportate. La codificazione di una gamma di diritti – in un certo senso – nuovi non costituisce semplicemente un approdo scritto per le corti in sede decisoria, ma comporta anche l'obbligo per il legislatore di predisporre una normativa che garantisca effettivamente l'esercizio e la tutela di quei diritti. Ciononostante, nello specifico settore della protezione dei dati a carattere personale, gli organi legislativi europei, se si esclude la normativa riguardante gli organismi e le istituzioni dell'Unione,[97] godevano di una competenza limitata all'armonizzazione delle normative nazionali relative

[95] PARISI N., *Funzione e ruolo della Carta dei diritti fondamentali nel sistema delle fonti alla luce del Trattato di Lisbona*, *op. cit*., pp. 653 e ss. Inoltre, secondo l'A., alle più ovvie conseguenze concernenti la maggiore certezza del diritto dell'Unione che derivano dall'articolato in esame, si aggiungono quelle relative all'affermazione della primazia del diritto europeo rispetto a quelli nazionali, atteso che la dotazione di uno statuto vincolante e gerarchicamente sovraordinato in materia di diritti fondamentali disinnesca eventuali istanze sollevate da corti costituzionali che, in ossequio alla teoria dei controlimiti, potrebbero circoscrivere l'applicabilità del diritto continentale in ragione del mancato rispetto dei principi fondamentali del proprio singolo ordinamento.

[96] *Ibid*., p. 664.

[97] L'art. 286 del Trattato che istituisce la Comunità europea (TCE) prescriveva al comma 1: "A decorrere dal 1° gennaio 1999 gli atti comunitari sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati si applicano alle istituzioni e agli organismi istituiti dal presente trattato o sulla base del medesimo". In virtù di tale disposizione, era stato adottato il Regolamento (CE) n. 45/2001 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 (Gazzetta ufficiale n. L 008 del 12/01/2001).

all'instaurazione ed al funzionamento del mercato interno. [98] Pertanto, era evidente ai redattori del Trattato di Lisbona che la svolta che stava intraprendendo l'organizzazione doveva necessariamente essere accompagnata da una innovazione delle sue competenze al fine, quantomeno, di prevenire la predisposizione di una protezione "monca" sin dalla nascita. [99]

In questo contesto si innesta il nuovo articolo 16 del Trattato sul funzionamento dell'Unione europea che appresta un fondamento giuridico nuovo e più idoneo alla attitudine costituzionalistica che aveva assunto la Carta di Nizza. [100] Dunque, come è stato correttamente sostenuto,[101] gli articoli 7 e 8 della Carta per quanto concerne la proclamazione di diritto sostanziale, e l'articolo 16 del TFUE, per quanto riguarda le competenze degli organi europei, rappresentano due facce della stessa medaglia consistente nella definitiva proclamazione e costituzionalizzazione del diritto alla protezione dei dati personali.[102]

Stante l'avallo del legislatore che aveva assecondato a livello normativo le istanze provenienti dalle corti europee, la giurisprudenza successiva all'entrata in vigore del Trattato di

[98] Nello specifico, si tratta dell'art. 100 A del TCE, sulla base del quale era stata adottata la Direttiva 95/46/CE.
[99] CALZOLAIO S., *Protezione dei dati personali*, *op. cit.*, pp. 619-620.
[100] L'art. 16 del TFUE recita: "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. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea".
[101] FIORILLO V., *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di Giustizia dell'Unione europea*, in *federalismi.it*, n. 15/2017, pp. 16-21.
[102] Per un approfondimento dettagliato in merito all'art. 16 TFUE si veda: HIJMANS H., *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU*, *op. cit*.

Lisbona si avvale con maggiore continuità e vigore dei principi sanciti dalla Carta dei diritti fondamentali, utilizzandoli quali parametro per valutare la legittimità delle norme di diritto derivato alla stregua di quanto accade nei tradizionali giudizi di costituzionalità nazionali.[103] Per altro verso però, è doveroso precisare che le motivazioni impiegate della Corte a sostegno delle proprie decisioni si agganciano ad una concezione quasi unitaria degli articoli 7 e 8 della Carta, dove, in alcuni casi, sembra che il secondo assuma rilievo solo in virtù del primo. Questo legame, derivante anche dall'influenza esercitata dalla Corte europea dei diritti dell'uomo che era "normativamente" costretta a attenervisi, è accentuato nella sentenza *Schecke* del 2010, dove il richiamo congiunto delle due disposizioni della Carta, unito al riferimento all'articolo 8 della CEDU,[104] tradiscono una più che comprensibile difficoltà di identificazione dei tratti differenziali della protezione dei dati personali in una vicenda relativa alla pubblicazione online del nominativo dei beneficiari di alcuni fondi europei in ossequio al principio di trasparenza.

Ad ogni modo, al di là di questo *Leitmotiv* che in misura più o meno marcata caratterizza tutte le sentenze della Corte *rationae materiae*, dall'analisi delle pronunce degli anni Dieci emerge prepotentemente il definitivo sorpasso del diritto alla protezione dei dati personali sulle libertà economiche, tanto da spingere la dottrina a esprimersi in termini di interpretazioni ai limiti della manipolazione del testo normativo e tendenti ad una assolutizzazione della protezione dei dati personali.[105] Sorprendentemente, tale esito

[103] CAGGIANO G., *La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali*, in *Studi sull'integrazione europea*, 2018, pp. 9 e ss.
[104] Corte di Giustizia, 9-11-2010, cause riunite C-92/09 e C-93/09, Volker und Markus Schecke GbR, par. 52.
[105] POLLICINO O., BASSINI M., *Commento all'art. 8 CdfUE, op. cit.*

non è ravvisabile solamente nelle decisioni in cui alla protezione dei dati personali (e della vita privata) si contrappongono interessi inerenti ad attività essenzialmente economiche, giacché anche l'interesse alla pubblica sicurezza è costretto a pagare dazio nel confronto con gli articoli 7 e 8 della Carta.

Ciò accade, innanzitutto, nella sentenza *Digital Rights Ireland* nel corso della quale la Corte arriva a dichiarare l'incompatibilità di un intero atto di diritto derivato con i principi fondamentali dell'ordinamento europeo.[106] La Direttiva 2006/24/CE riguardante, come visto in precedenza, 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, permetteva agli Stati membri di implementare misure volte ad imporre ai fornitori di servizi l'obbligo di conservare, indiscriminatamente e per un periodo di massimo due anni, tutti i dati concernenti le comunicazioni telefoniche o telematiche, eccetto quelli relativi al contenuto di tali comunicazioni,[107] ai fini di indagine, accertamento e perseguimento di reati gravi. La mancanza di criteri volti a distinguere le ragioni che motivano la conservazione di determinati tipi di dati personali, spingono la Corte ad appurare il mancato rispetto di (parte) dell'articolo 52 delle Carta dei diritti fondamentali dell'Unione, il quale, nel prescrivere le condizioni al ricorrere delle quali i diritti in essa sanciti possono essere legittimamente sottoposti a limitazioni, impone il rispetto del contenuto essenziale del diritto e dei principi di necessità e proporzionalità.[108] La decisione della Corte si sviluppa sulla falsariga

[106] Corte di Giustizia, 8-4-2014, cause riunite C-293/12 e C-594/12, Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural resources et al.
[107] Art. 5, Direttiva 2006/24/CE.
[108] L'art. 52, c. 1 della Carta recita: "Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il

di un giudizio di legittimità costituzionale, dove la Carta assurge al ruolo di statuto di rango primario in raffronto al quale vanno valutate le disposizioni subordinate, e si conclude con la dichiarazione di invalidità della direttiva in questione sulla base proprio del mancato rispetto del superiore principio di proporzionalità.[109]

L'approccio espansivo attraverso il quale la Corte incrementa la propagazione degli effetti della Carta è percepibile in maniera ancor più evidente nella successiva sentenza *Tele2 Sverige*, quando i principi affermati in occasione della sentenza *Digital Rights Ireland* riescono a trovare applicazione anche nei confronti delle normative nazionali che hanno dato attuazione alla Direttiva 2006/24/CE.[110] In particolare, nel corso di due vicende nate dalla contestazione dell'obbligo di conservazione imposto ai fornitori di servizi di comunicazione per mezzo di leggi statali, viene dissipato ogni dubbio in merito alla portata delle prescrizioni previste dalla Carta – nel caso di specie degli articoli 7, 8 e 52 – le quali non vincolano in via diretta esclusivamente il legislatore europeo, ma anche quelli nazionali.

---

contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui".

[109] Corte di Giustizia, cause riunite C-293/12 e C-594/12, Digital Rights Ireland, par. 69. La Corte di giustizia ravvisa il mancato rispetto del requisito di proporzionalità in quanto la Direttiva 2006/24/CE "riguarda in maniera generale qualsiasi persona e qualsiasi mezzo di comunicazione elettronica nonché l'insieme dei dati relativi al traffico senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi" (par. 57), "non prevede alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore" (par. 60), "impone, all'articolo 6, la conservazione degli stessi per un periodo di almeno sei mesi senza che venga effettuata alcuna distinzione tra le categorie di dati previste all'articolo 5 della direttiva a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate […] senza che venga precisato che la determinazione della durata di conservazione debba basarsi su criteri obiettivi al fine di garantire che sia limitata allo stretto necessario" (parr. 63-64) e, infine, "non prevede garanzie sufficienti, come richieste dall'articolo 8 della Carta, che permettano di assicurare una protezione efficace dei dati conservati contro i rischi di abuso nonché contro eventuali accessi e usi illeciti dei suddetti dati" (par. 66).

[110] Corte di Giustizia, 21-12-2016, cause riunite C-203/15 e C-698/15, Tele 2 Sverige AB *c*. Post-och telestyrelsen.

Per quanto concerne la contrazione che l'interesse alla pubblica sicurezza è costretto a patire rispetto alla protezione dei dati personali e della vita privata,[111] la celebre sentenza *Schrems* ricopre un ruolo fondamentale in quanto ha permesso al diritto europeo di fare un salto in avanti anche dal punto di vista "geografico".[112] Se l'obbligo del rispetto degli articoli 7 e 8, nel significato attribuitogli dalla Corte, era stato prescritto prima nei confronti del legislatore europeo, con la decisione *Digital Rights Ireland*, e poi nei confronti di quello nazionale, con la successiva decisione *Tele2 Sverige*; ora la sentenza *Schrems* sembra prendere di mira, anche se in maniera necessariamente più mitigata, il legislatore straniero. Di nuovo, un intervento deciso della giurisprudenza arriva ad invalidare un atto di diritto comunitario derivato, segnatamente, la decisione n. 2000/250 con cui la Commissione aveva ritenuto idoneo il cosiddetto "*Safe Harbour*", ossia l'accordo tra Unione europea e Stati Uniti d'America per mezzo del quale veniva garantita la liceità del trasferimento di dati tra le due sponde dell'oceano. A seguito della scoperta dei programmi di sorveglianza implementati dalle autorità di sicurezza statunitensi, il ricorso del cittadino austriaco Maximilian Schrems contestava che l'accordo *Safe Harbour* fosse in grado di assicurare un livello di tutela per i dati personali paragonabile a quello europeo. Dopo aver stabilito la propria competenza a sindacare la compatibilità degli atti della Commissione con le norme europee di rango fondamentale, la Corte, nell'affermare che il fine della disciplina continentale rimane altresì quello di assicurare la

[111] OROFINO M., *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in PANELLA L., *Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno. Quaderni Ordine Internazionale e Diritti Umani Editoriale Scientifica*, Napoli, 2018, 245-268.
[112] Corte di Giustizia, 6-10-2015, causa C-362-14, Maximilian Schrems *c*. Data Protection Commissioner.

continuità nella protezione dei dati personali anche in caso di uscita dal territorio europeo, [113] stabilisce che la discordanza fra l'ordinamento europeo e quello statunitense è troppo ampia per poter essere tollerata.[114] Peraltro, non si tratta semplicemente di porre un freno all'incontrollato accesso alle informazioni personali dei cittadini europei perpetrato dalle autorità americane, ma in un certo qual modo, sembra che la Corte stia tentando di estendere l'ambito di applicazione del diritto dell'Unione anche ad ordinamenti extra-comunitari, imponendo per l'appunto un livello di adeguatezza che suona più come una richiesta di equivalenza.[115]

Questo filone giurisprudenziale che rinviene una chiara primazia del diritto alla protezione dei dati personali rimane granitico anche quando il bilanciamento deve essere fatto rispetto a diritti e interessi di carattere economico. Nella storica sentenza *Google Spain*, [116] la Corte stabilisce, simultaneamente e con una evidente creatività esegetica, un insieme di principi che sono destinati a cambiare il futuro della regolamentazione del trattamento dei dati personali. [117] Si delinea per la prima volta

[113] *Ibid*., par. 72.
[114] RESTA G., *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in RESTA, ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Collana "Consumatori e Mercato", 2016, pp. 23 e ss.
[115] POLLICINO O., BASSINI M., *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in RESTA, ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Collana "Consumatori e Mercato", 2016, pp. 73 e ss.
Successivamente, con la sentenza del 16/07/2020 nella causa C-311/18. (Data Protection Commissioner *c*. Facebook Ireland Limited e Maximillian Schrems), nota come *Schrems* II, la Corte ha invalidato di nuovo la decisione (n. 2016/1250) con cui la Commissione europea aveva constatato l'adeguatezza della protezione dei dati personali fornita dal "*Privacy Shield*", ossia il regime per lo scambio di dati approvato in seguito alla invalidazione del "*Safe Harbour*".
[116] Corte di Giustizia, 13-5-2014, causa C-131/12, Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González.
[117] La rilevanza sancita dagli elementi presenti in questa sentenza è testimoniata dalla loro successiva inclusione nel Regolamento 2016/679.

quell'atteggiamento ostruzionistico nei confronti dei motori di ricerca, e in generale delle *big tech* estere,[118] che caratterizzerà il percorso giuridico europeo negli anni successivi. Il primo fendente della Corte arriva dalla qualificazione di titolare del trattamento del motore di ricerca, alla quale non fa però seguito un correlativo riconoscimento del perseguimento di scopi giornalistici o di espressione artistica o letteraria, che, a mente dell'articolo 9 della Direttiva 95/46/CE, avrebbe consentito a Google di fare affidamento sulle esenzioni o deroghe "per conciliare il diritto alla vita privata con le norme sulla libertà d'espressione" che gli Stati membri erano obbligati a prevedere.[119] Oltretutto, per quanto attiene all'influenza esterna che i giudici contribuiscono a conferire al diritto europeo, la sentenza interviene anche sul campo di applicazione della disciplina. Viene statuito chiaramente che gli obblighi gravanti sui titolari del trattamento vigono anche nei confronti di soggetti che hanno lo stabilimento principale situato in un Paese terzo, quantomeno in tutti quei casi in cui il titolare del trattamento disponga di una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari in uno Stato membro, indirizzando la propria attività verso gli abitanti di tale Stato membro.[120] D'altro canto, la spinta riformista innescata dai giudici approda anche sul versante opposto, quello dell'interessato. Tramite una interpretazione evolutiva dell'articolo 12, lett. b) della Direttiva 95/46/CE, relativo al diritto

[118] Per un inquadramento giuridico dei servizi OTT e, in generale, per una disamina della tensione tra libertà di espressione e innovazione tecnologica, si veda: OROFINO M., *La libertà di espressione tra Costituzione e Carte europee dei diritti. Il dinamismo dei diritti in una società in continua trasformazione*, Giappichelli, Torino, 2014.
[119] Corte di Giustizia, causa C-131/12, Google Spain SL, par. 85.
[120] *Ibid*., parr. 49-60. In particolare, La Corte fa leva su un'interpretazione estensiva dell'inciso "nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro" all'art. 4, par. 1, lett. a), della Direttiva 95/46, al preciso scopo di garantire una tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche.

di rettifica, cancellazione o congelamento dei dati il cui trattamento non sia conforme alla normativa, viene riconosciuto all'individuo un diritto alla deindicizzazione, ossia la facoltà di chiedere al motore di ricerca la rimozione, dall'elenco di risultati prodotti in seguito ad una ricerca effettuata a partire dal suo nome, dei *link* verso pagine *web* legittimamente pubblicate da terzi e contenenti informazioni veritiere riguardanti il richiedente. Nella parte motiva della sentenza, non solo viene disattesa l'obiezione secondo la quale l'istanza sarebbe dovuta essere rivolta solamente all'editore del sito *web*, ma la Corte dà una lettura così estensiva del requisito dell'incompatibilità con la direttiva previsto dalla lettera b) dell'articolo 12, da rendere legittime le richieste di cancellazione senza che sia necessario valutare un eventuale pregiudizio patito dall'interessato a causa della pubblicazione del *link*.[121] A ben vedere, la supremazia dei diritti individuali stabilita dalla pronuncia in parola non concerne solamente il confronto con le libertà economiche, ma, trattandosi di un motore di ricerca il cui scopo rimane quello di organizzare e rendere disponibili dati, è lo stesso interesse collettivo all'ottenimento delle informazioni a risultare soccombente. I giudici si dimostrano consapevoli del rischio sotteso al bilanciamento dei diritti dell'individuo con il legittimo interesse degli utenti di internet potenzialmente interessati ad accedere alle informazioni, ma costruiscono il loro giudizio sulla base di una presupposta prevalenza dei diritti del singolo su quelli della collettività, salvo circostanze eccezionali in cui la natura dell'informazione, la sua sensibilità e l'interesse del pubblico giustifichino una soluzione inversa. Invero,

[121] *Ibid*., parr. 92-99. Per dovere di precisione, è opportuno sottolineare che al *data subject* viene garantita la possibilità di chiedere la rimozione del collegamento che dalla pagina *web* del motore di ricerca rimanda ad una determinata fonte di informazioni (sito *web* dell'editore). Peraltro, tale prerogativa non consente di chiedere – quantomeno al motore di ricerca – la rimozione dei dati dalla fonte medesima.

il ragionamento della Corte sembra fungere, in parte, da "specchietto per le allodole" nella misura in cui permette di porsi al riparo da eventuali obiezioni in merito alla eccessiva compressione del diritto ad informare ed essere informati, che trova dimora solamente come eccezione fondata sul particolare ruolo di figura pubblica ricoperto da determinati interessati.[122]

La conferma di questa diffidenza dell'Europa nei confronti delle *big tech* sembra trovare parziale conferma, *a contrario*, nella più recente sentenza Manni.[123] La vicenda nasce da un ricorso proposto nel 2007 da Salvatore Manni, amministratore unico di una società a responsabilità limitata operante nel settore immobiliare, avverso la Camera di commercio di Lecce, per avere quest'ultima negato l'istanza di cancellazione di dati personali avanzata dall'interessato. Nello specifico, l'attore lamentava che la notizia dell'intervenuto fallimento di un'altra S.r.l da lui precedentemente amministrata, dichiarato nel 1992, pregiudicasse la sua libertà di iniziativa economica e la possibilità di assicurarsi nuova clientela. In questa occasione, la Corte ha negato la sussistenza di un obbligo per gli Stati membri di garantire agli individui interessati il diritto di ottenere la cancellazione dei dati personali decorso un determinato periodo di tempo dallo scioglimento della società da essi gestita sulla base di un duplice ordine di ragioni. In primo luogo, la pubblicazione di quei dati personali sul registro delle imprese era prevista da una direttiva comunitaria del 1968,[124] avente lo scopo di tutelare gli

[122] *Ibid*., parr. 81 e 97.
[123] Corte di giustizia, 9-03-2017, causa C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce *c*. Salvatore Manni.
[124] Si tratta della Prima direttiva 68/151/CEE del Consiglio, del 9 marzo 1968, intesa a coordinare, per renderle equivalenti, le garanzie che sono richieste, negli Stati Membri, alle società a mente dell'articolo 58, secondo comma, del Trattato per proteggere gli interessi dei soci e dei terzi (Gazzetta ufficiale n. L 65 del 14/03/1968), come modificata dalla direttiva 2003/58/CE, del Parlamento europeo e del Consiglio, del 15 luglio 2003 (Gazzetta ufficiale n. L 221 del 4/09/2003).

interessi dei terzi assicurando loro la conoscenza degli atti essenziali delle società per azioni e delle società a responsabilità limitata, la cui garanzia è circoscritta al relativo patrimonio sociale.[125] In secondo luogo, viene sostenuto che "l'esigenza di tutelare gli interessi dei terzi nei confronti delle società per azioni e delle società a responsabilità limitata e di garantire la certezza del diritto, la lealtà delle transazioni commerciali e, quindi, il buon funzionamento del mercato interno", dunque argomenti di carattere prettamente economico, giustifica un'ingerenza nei diritti sanciti dagli articoli 7 e 8 della Carta, valutata come legittima in quanto rispettosa del principio di proporzionalità.[126] La Corte conclude – e, visti i risvolti della sentenza *Google Spain*, non avrebbe potuto fare altrimenti – aprendo alla possibilità di limitare, in via eccezionale, l'interesse pubblico correlato alla redazione del registro delle imprese quando ricorrono "situazioni particolari in cui ragioni preminenti e legittime connesse al caso concreto della persona interessata giustifichino, in via eccezionale, che l'accesso ai dati personali ad essa relativi iscritti nel registro sia limitato", specie nelle ipotesi in cui è intercorso un cospicuo lasso di tempo dalla dichiarazione di fallimento, secondo una valutazione rimessa alla discrezionalità politica dei singoli legislatori nazionali.[127]

Le motivazioni della sentenza sembrano restituire una Corte che torna ad essere paladina del mercato unico e che pondera i diritti e gli interessi che emergono in corso di causa senza posizioni

[125] Corte di giustizia, causa C-398/15, Manni, *cit*., parr. 49-55.
[126] *Ibid*., par. 59.
[127] *Ibid*., par. 60 e ss. Nell'ipotesi in cui il legislatore abbia predisposto una normativa che consente istanze di cancellazione dal registro delle imprese, spetterà poi al giudice "valutare, alla luce dell'insieme delle circostanze rilevanti e tenuto conto del termine decorso dopo lo scioglimento della società interessata, l'eventuale esistenza di ragioni preminenti e legittime che sarebbero, se del caso, tali da giustificare, in via eccezionale, una limitazione all'accesso di terzi".

assolutiste, ma sulla base di ragioni fattuali concrete. Si potrebbe ritenere che il ribaltamento di prospettiva rispetto a quanto avvenuto tre anni prima nel caso *Google Spain* sia motivato dalle sottili differenze che intercorrono tra le due vicende da cui sono sorte le questioni di pregiudizialità su cui si è pronunciata la Corte. Se nella sentenza del 2014 il rilievo ricoperto dall'elemento tecnologico-digitale aveva un'incidenza di gran lunga maggiore ed il *decisum* dei giudici si focalizzava specificamente sulla deindicizzazione, nella sentenza Manni il *petitum* era circoscritto alla cancellazione dell'informazione dalla fonte originale, indipendentemente dal suo formato digitale o analogico, da parte di una autorità pubblica. A ben vedere però, la precedenza accordata all'interesse pubblico all'accesso dell'informazione, con la conseguente soccombenza dell'interesse individuale del ricorrente, appare riflettere una presa di distanza netta della Corte dalle pratiche dei motori di ricerca e di chiunque gestisce enormi moli di informazioni in maniera centralizzata, ossia di tutti quei soggetti, pubblici o privati, che potrebbero interferire nell'ordinamento eurounitario dall'esterno.

In conclusione della testé esposta disamina delle pronunce della Corte di giustizia, è possibile svolgere qualche osservazione più precisa in materia di applicazione della Carta dei diritti fondamentali dell'Unione e, nello specifico, delle norme relative al trattamento dei dati a carattere personale.

Innanzitutto, pare oramai corretto affermare senza timore di smentita che la protezione dei dati personali ha assunto la veste di diritto di rilievo costituzionale all'interno dell'ordinamento giuridico europeo. Oltretutto, si tratta di una fattispecie che, ad opinione della giurisprudenza, ricopre un rilievo così decisivo da introdurre una sorta di gerarchizzazione fra i diritti annoverati dalla Carta dei diritti fondamentali – non presente nel documento – e che comunque

permette alla protezione dei dati personali (e al rispetto alla vita privata) di uscire sostanzialmente illesa dal confronto con interessi che nella società continentale moderna hanno un livello di prim'ordine, come la sicurezza pubblica, il diritto di informazione e la libertà di iniziativa economica.[128] A tale proposito, occorre comunque mettere in evidenza che il processo di progressiva acquisizione di autonomia rispetto alla tutela della vita privata non ha ancora raggiunto un traguardo definitivo in ambito giurisprudenziale, giacché le pronunce della Corte dimostrano ancora una carenza di uniformità di vedute. Come è stato correttamente notato,[129] la distinzione in questione fatica ad emergere anche a causa dei problemi definitori che circondano la fattispecie del dato personale e che si sono in parte amplificati, come si vedrà nel prosieguo, dopo che il legislatore continentale ha deciso di regolamentare anche il versante dei dati non personali.

Una volta che il dialogo tra corti e legislatore europei ha portato all'abbandono della prospettiva che voleva la protezione dei dati personali inscindibilmente connessa con le libertà economiche previste dati trattati istitutivi della Comunità europea, la Carta ha trovato un'applicazione e una diffusione quasi inaspettata. L'intensità del suo impatto è tangibile in quelle pronunce in cui la Corte propone una rilettura alla luce degli articoli 7 e 8 di normative entrate in vigore antecedentemente al 2009. Tale sforzo esegetico, ai limiti della manipolazione, propone una interpretazione invertita, valutando disposizioni di diritto derivato già vigenti come declinazione puntuale di un atto successivo,[130] e conducendo spesso

[128] POLLICINO O., BASSINI M., *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo, op. cit.*, p. 90.
[129] ROSSI DAL POZZO F., *La giurisprudenza della Corte di giustizia sul trattamento dei dati personali, op. cit.*, pp. 140-143.
[130] POLLICINO O., BASSINI M., *Commento all'art. 8 CdfUE, op. cit.*

ad una supremazia quasi intrinseca alla protezione dei dati nei confronti di altri diritti o interessi contrapposti.[131]

Una analisi delle decisioni della Corte di giustizia che va al di là del dato letterale suggerisce che la volontà, quasi politica,[132] dei giudici sia stata guidata da due obiettivi principali. In primo luogo, la visione costantemente protesa in avanti dimostra una palese intenzione di adattamento all'avanzare delle nuove tecnologie che hanno la capacità di insidiarsi nelle sacche lasciate vuote da un diritto vetusto e rimasto ancorato a un modello di gestione dei dati che non rispecchia più la realtà dei fatti. In secondo luogo, la barriera innalzata dalla Corte rispetto alle possibili ingerenze esterne, specie nei casi *Google Spain* e *Schrems,* sembra essere concepita come l'unica via al momento percorribile dall'Unione europea per difendersi dall'annientamento tecnico che sta patendo tanto sul versante occidentale quanto su quello orientale. I rischi di perdita di sovranità e di rilievo geopolitico che sta fronteggiando il vecchio continente impongono il ricorso a rimedi di pronto utilizzo che, allo stato dell'arte, possono rinvenirsi solamente nello strumentario giuridico, in attesa di positivi e magari più celeri sviluppi di quello tecnologico.[133]

---

[131] FIORILLO V., *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di Giustizia dell'Unione europea*, *op. cit*., pp. 16-21.

[132] FINOCCHIARO G., *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a* Schrems, in RESTA, ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Collana "Consumatori e Mercato", 2016, pp. 115-117.

[133] ZENO-ZENCOVICH V., *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in RESTA, ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Collana "Consumatori e Mercato", 2016, pp. 7-9.

6. La normativa vigente: il Regolamento (UE) 2016/679 e il Regolamento (UE) 2018/1807 (*cenni*)

Il cammino seguito dall'Europa nella delicata operazione di modellamento del quadro giuridico in materia di dati si conclude con la fase attuale, quella che sancisce in via definitiva una spaccatura nella catalogazione dei dati. Attualmente vigono due diversi regolamenti che disciplinano, rispettivamente, la categoria dei dati personali, nella quale assumono rilievo sia la protezione degli stessi sia la loro circolazione, e la categoria dei dati non personali, dove le norme hanno ad oggetto (quasi) esclusivamente la dimensione del libero flusso. Prima dell'analisi comparativa fra le due discipline dal punto di vista delle regole e degli effetti che le stesse producono nei confronti della circolazione, oggetto del capitolo successivo, è opportuno illustrare brevemente gli elementi fondamentali di ognuna di esse.

Il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (in inglese *General Data Protection Regulation*, o GDPR) procede all'abrogazione della precedente Direttiva 95/46/CE, [134] senza tuttavia travolgerne totalmente l'impostazione di fondo. Come anticipato, il Regolamento in esame arricchisce quanto già previsto dalla Direttiva Madre, accogliendo le richieste e le indicazioni che la Corte di giustizia aveva segnalato per mezzo delle sentenze pronunciate nel contesto della previgente normativa. [135] Ad esempio, per la definizione

[134] 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.
[135] STANZIONE M. G., *Genesi ed ambito di applicazione*, in SICA S., D'ANTONIO V., RICCIO G., *La nuova disciplina europea della privacy*, 2016, pp. 13-31.

dell'ambito di applicazione territoriale, l'articolo 3 riflette in maniera evidente la volontà di allargare il perimetro di validità della disciplina in ossequio a quanto stabilito in via pretoria, giacché introduce due condizioni alternative – nella specie, quando gli interessati che si trovano in territorio europeo sono destinatari dell'offerta di beni o servizi o quando il loro comportamento è oggetto di monitoraggio – al ricorrere delle quali gli obblighi del GDPR si impongono anche a chi è stabilito al di fuori dell'Unione. La stessa logica è stata adottata per la redazione dell'articolo 17, rubricato "diritto alla cancellazione («diritto all'oblio»)", il quale rappresenta la trasposizione normativa di quanto predicato dalla Corte di giustizia nella sentenza *Google Spain*.[136] La facoltà, condizionata,[137] di ottenere la cancellazione dei propri dati personali e, soprattutto,[138] la correlativa previsione di un obbligo per il titolare del trattamento di adottare misure ragionevoli per informare gli altri titolari che stanno trattando i dati personali oggetto della richiesta della necessità di cancellare qualsiasi *link*, copia o riproduzione sembrano disposizioni appositamente ritagliate per il settore dei motori di ricerca e dei grandi gestori di dati in generale.[139]

Per altro verso, però, il regolamento mostra il suo vero carattere innovatore nella parte in cui trasferisce in maniera più decisa la responsabilità del trattamento dei dati in capo a coloro che

[136] ALLEGRI M. R., *Diritto all'oblio, tutela della web reputation individuale e "eccezione giornalistica": spunti giurisprudenziali*, in *Forum di Quaderni Costituzionali*, 2018.
[137] Il par. 1 dell'art. 17 del GDPR consente l'esercizio del diritto all'oblio se ricorre una delle seguenti condizioni: a) i dati personali non sono più necessari rispetto alle finalità originali; b) l'interessato revoca il consenso su cui si basa il trattamento; c) l'interessato si oppone al trattamento; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo legale; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.
[138] FINOCCHIARO G., *Il diritto all'oblio nel quadro dei diritti della personalità*, in RESTA G., ZENO-ZENCOVICH V., (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Collana "Consumatori e Mercato", 2015, pp. 29 e ss.
[139] Art. 17, par. 2, GDPR.

ne hanno effettivamente il controllo, ossia il titolare ed il responsabile. La partita non si gioca solamente sul versante di un interessato che deve essere vigile nell'esercitare in maniera puntuale i diritti che gli vengono riconosciuti, ma vengono valorizzati in misura significativa i correlativi doveri e oneri gravanti sui soggetti che effettuano il trattamento.[140] Per il tramite di questa apprezzabile mossa, il legislatore europeo fornisce una possibile soluzione alle necessità di adeguamento della disciplina a un nuovo modello di gestione dei dati rispondente a logiche non sempre note ai *data subject*, i quali rimangono spesso bersagli inconsapevoli di trattamenti eseguiti sulle loro informazioni. L'idea che ha guidato i redattori del testo definitivo è stata principalmente quella di aumentare la tutela attraverso una sua anticipazione, ossia collocandola in un momento anteriore alla mera fase riparatoria e successiva che può competere all'interessato. A questa strategia si ricollegano tanto la previsione dei principi di *privacy by design* e *privacy by default*, introdotti dall'articolo 25 del GDPR,[141] quanto la valutazione d'impatto sulla protezione dei dati personali, prevista dall'articolo 35.[142]

---

[140] PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali, I, Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, pp. 153 e ss.

[141] Il primo dei due principi prescrive la necessità per il titolare del trattamento di integrare, a monte, nella fase di *design* del trattamento una serie di garanzie idonee ad implementare le misure tecniche e organizzative, disponibili allo stato dell'arte, al fine di dare concreta attuazione ai principi di protezione dei dati sanciti dal GDPR. Similmente, anche il principio di *privacy by default* mira ad assicurare il rispetto della disciplina, ma sembra promuovere un autentico cambio di prospettiva da parte dei titolari del trattamento, i quali devono mettere in atto misure tecniche ed organizzative dirette a limitare la quantità, la conservazione e l'accessibilità dei dati elaborati "per impostazione predefinita". Per un approfondimento, si vedano: CAVOUKIAN A., *7 foundational principles of privacy by design*, Office of the Information & Privacy Commissioner of Ontario, 2010; CALZOLAIO S., *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in *federalismi.it*, n. 24/2017, pp. 1-21.

[142] L'istituto della valutazione d'impatto rappresenta una caratteristica distintiva del nuovo Regolamento europeo e costituisce il frutto dell'approccio basato sul rischio che permea l'intera disciplina. Difatti, tale valutazione viene svolta al preciso scopo di determinare "l'origine, la natura, la particolarità e la gravità di tale rischio", per poi procedere, sulle base

La volontà di ristrutturare l'impianto in chiave moderna è percepibile anche grazie ad altri istituti che fanno la loro comparsa sul panorama continentale proprio per merito del GDPR. Fra questi, il cosiddetto "*risk based approach*" si è rivelato un formidabile strumento per conferire rilievo normativo nel contesto della nuova infrastruttura regolamentare all'assunto secondo cui il *data subject* non è in grado né di avere piena contezza dell'entità dei rischi connaturati alla circolazione dei dati che lo riguardano, né di gestirli autonomamente.[143] Dunque, le nuove regole in materia di dati personali si fanno portatrici di un cambio di paradigma nella amministrazione e mitigazione del rischio, trasferendo parte degli oneri derivanti dal trattamento dei dati in capo a soggetti diversi dal singolo interessato, secondo un'impostazione dinamica che impone un costante monitoraggio delle esternalità negative derivanti dalle modalità con cui tale trattamento viene eseguito.[144]

Detta svolta, se da un lato si è tradotta nella stesura di norme completamente nuove, come quelle relative alla citata valutazione d'impatto o all'introduzione della figura del Responsabile per la protezione dei dati personali;[145] dall'altro lato, ha portato ad una rilettura "in chiave digitale" di disposizioni che erano già presenti nella Direttiva 95/46/CE e che sono state riprodotte nel regolamento

---

delle risultanze di tale esame, alla selezione delle misure più idonee a mitigarlo. Per un approfondimento in materia, si vedano le "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" (WP 248) adottate dal Gruppo di lavoro Articolo 29 il 4 aprile 2017 e modificate il 4 ottobre 2017.

[143] MANTELERO A., *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le Nuove Leggi Civili Commentate*, n. 1/2017, pp. 144 ss.

[144] COLAPIETRO C., *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *federalismi.it*, n. 2/2018, pp. 1-34.

[145] A tale riguardo, si rimanda alle "Linee-guida sui responsabili della protezione dei dati (RPD)" (WP 243) adottate dal Gruppo di lavoro Articolo 29 il 13 dicembre 2016 e modificate il 5 aprile 2017.

del 2016. I principi di liceità, finalità, esattezza e minimizzazione, già contemplati nell'articolo 6 della direttiva, acquisiscono un significato diverso nell'era della datificazione, degli algoritmi, e dei *Big Data* dove è necessario uno sforzo interpretativo notevole per riuscire nell'intento di conciliare la predeterminazione dello scopo del trattamento e la limitazione della conservazione con la natura mutevole e in costante evoluzione della realtà digitale.[146]

Un ulteriore precipitato della rivisitata concezione di rischio presente nel regolamento interessa anche le condizioni che legittimano l'esecuzione del trattamento. Ora, l'articolo 6 sembra certificare l'avvenuto superamento della centralità del modello informativa-consenso che contraddistingueva la previgente normativa in favore di una sostanziale parificazione di tutte le basi giuridiche idonee a conferire liceità al trattamento in un'ottica, per l'appunto, di modifica di un paradigma non più adeguato alla realtà digitale del XXI secolo.[147]

Nella mente degli organi che hanno partecipato alla realizzazione del GDPR, all'obiettivo di ammodernamento si aggiungeva anche quello di uniformazione delle regole fra i vari Paesi componenti l'Unione.[148] La transnazionalità delle nuove tecnologie, unita ai deludenti risultati raggiunti dalle discipline

---

[146] MAYER-SCHÖNBERGER V., PADOVA Y., *Regime Change? Enabling Big Data through Europe's New Data Protection Regulation*, in *The Columbia Science & Technology Law Review*, 2016, pp. 323 e ss.; ZARSKY T., *Incompatible: The GDPR in the Age of Big Data*, in *Seton Hall Law Review*, vol, 47, n. 995, 2017, pp. 1005-1009.

[147] MANTELERO A., *Responsabilità e rischio nel Reg. UE 2016/679*, *op. cit.*

[148] Per i profili relativi all'armonizzazione della tutela giurisdizionale e il potenziale conflitto con la disciplina della giurisdizione nelle controversie civili e commerciali, si veda: MARONGIU BUONAIUTI F., *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I-bis"*, in *Cuadernos de Derecho Transnacional*, vol. 9, n. 2, 2017, pp. 448-464.

statali dal punto di vista dell'armonizzazione,[149] hanno suggerito alle istituzioni di prediligere l'opzione del regolamento in luogo della direttiva, la quale, come strumento normativo, si dimostra spesso inadatto nelle ipotesi di regolamentazione della tecnologia.[150] Lo stesso preambolo del GDPR certifica l'insostenibilità della frammentazione "dell'applicazione della protezione dei dati personali nel territorio dell'Unione", in quanto tanto il "divario creatosi nei livelli di protezione", quanto gli ostacoli alla libera circolazione dei dati essenziale per l'economia europea sono dovuti "alle divergenze nell'attuare e applicare la direttiva 95/46/CE".[151] Da tale premessa mutua la scelta di optare per una fonte di diritto capace di "assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione".[152]

Una volta che il progresso normativo europeo si è finalmente rivelato nella sua essenza, attraverso l'approvazione di uno fra i più rilevanti atti di diritto derivato della storia recente, la vocazione delle istituzioni eurounitarie alla regolazione della tecnologia non poteva considerarsi esaurita con l'entrata in vigore di un impianto giuridico votato alla disciplina del solo dato a carattere personale. Pertanto, il legislatore europeo, preso atto dell'incompletezza di una normativa di settore focalizzata solamente su una parte del tutto, ha rivolto il suo interesse all'economia dei dati nella sua interezza e ha introdotto un ulteriore tassello affinché venisse completato il "quadro globale

[149] VOIGT P., VON DEM BUSSCHE A., *The EU General Data Protection Regulation (GDPR): A Practical Guide*, *op. cit*.
[150] Ad esempio, si inserisce in tale *trend* anche la (da tempo avviata e non ancora terminata) sostituzione della Direttiva 2002/58/CE con un nuovo Regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche.
[151] Regolamento (UE) 2016/679, cons. n. 9.
[152] Regolamento (UE) 2016/679, cons. n. 10.

per uno spazio comune europeo dei dati e per la libera circolazione di tutti i dati all'interno dell'Unione europea".[153]

Il Regolamento (UE) 2018/1807 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea (Regolamento 1807 o RDNP)[154] costituisce il primo atto legislativo continentale contenente una definizione di dati non personali. Facendo riserva di svolgere nel capitolo terzo gli opportuni approfondimenti in merito alle questioni definitorie, per apprezzare appieno la ratio del Regolamento 1807, è necessario porre attenzione, *in primis*, alla sua base giuridica. Mentre, come è noto, il GDPR si fonda sull'articolo 16 del TFUE, il regolamento più recente poggia sull'articolo 114 del TFUE, il quale attribuisce al Parlamento ed al Consiglio la competenza di armonizzazione al fine di ravvicinare le norme nazionali che rappresentano un ostacolo alla libera circolazione. Dunque, si tratta di una norma strumentale al raggiungimento di un obiettivo che, benché di notevole rilevanza, non è suscettibile di prevalere sui principi e sui diritti sanciti dalla Carta dei diritti fondamentali dell'Unione europea. Dal confronto tra le due disposizioni emerge che, da una parte, l'articolo 16 considera preminente il diritto alla protezione dei dati personali rispetto alla libera circolazione – la quale, comunque, non scompare dall'orbita di interesse della norma –;[155] dall'altra parte, l'articolo 114 è imperniato esclusivamente su questa seconda dimensione: il combinato disposto delle due basi giuridiche suggerisce, dunque, che

[153] Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union* (COM (2019) 250 final), p. 2.
[154] 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 (Gazzetta ufficiale n. L 303 del 28/11/2018).
[155] A tale proposito, è utile ricordare che il principio di libera circolazione intra-europea dei dati personali rimane una caratteristica essenziale del GDPR.

l'ordinamento europeo tutela entrambi i valori in gioco, ma non in modo paritario. La residualità dell'applicazione del regolamento sui dati non personali rispetto a quello sui dati personali rappresenta il precipitato logico di questo ragionamento: la circolazione dopo la protezione.[156]

Ad ogni modo, trattandosi di un impianto regolamentare attento principalmente alla dimensione economica del flusso dei dati, tanto la definizione quanto la disciplina del dato non personale del Regolamento 1807 sono state plasmate in maniera tale da soddisfare al meglio le esigenze di libera circolazione all'interno dell'Unione. Pertanto, fra i vari aspetti che interessano l'economia dei dati, il legislatore europeo ha ritenuto opportuno concentrarsi su quelli che più di ogni altro hanno un "*chilling effect*" sulla possibilità di trasferire le informazioni nel mondo digitale: gli obblighi di localizzazione dei dati, la messa a disposizione dei dati alle autorità di controllo e, infine, la portabilità dei dati per gli utenti professionali.[157]

Gli obblighi di localizzazione consistono, secondo quanto stabilito dall'articolo 3, punto 5, del RDNP, in disposizioni di legge, orientamenti o pratiche amministrative che, direttamente o indirettamente, impongono di effettuare il trattamento dei dati non personali nel territorio di un determinato Stato membro o che ne ostacolano il trattamento in un altro. Dal momento in cui numerose

---

[156] ROSSI DAL POZZO F., *La giurisprudenza della Corte di giustizia sul trattamento dei dati personali*, *op. cit.* p. 134.
Inoltre, come ulteriore conferma, è sufficiente guardare all'articolo 44 del GDPR, il quale, nel definire il principio generale in materia di trasferimenti transfrontalieri di dati personali, conclude affermando che: "tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato".

[157] L'articolo 1 del RDNP recita: "Il presente regolamento mira a garantire la libera circolazione dei dati diversi dai dati personali all'interno dell'Unione stabilendo disposizioni relative agli obblighi di localizzazione dei dati, alla messa a disposizione dei dati alle autorità competenti e alla portabilità dei dati per gli utenti professionali".

analisi hanno dimostrato quanto l'economia dei dati europea possa trarre beneficio da uno scambio più intenso di informazioni tra Stati membri,[158] l'articolo 4 impone un divieto generale di introduzione o mantenimento di tali misure restrittive alla circolazione, salvo che siano giustificate da motivi di sicurezza pubblica.[159]

L'articolo 5, invece, risponde alla seria preoccupazione, espressa a più riprese in seno alle consultazioni che hanno preceduto l'approvazione del regolamento, relativa all'eventuale abuso del diritto a trasferire i dati all'estero da parte dei titolari al solo fine di impedire, o quantomeno rallentare, le verifiche delle autorità di controllo nazionali.[160] Di conseguenza, nell'intento di evitare che una nuova opportunità di crescita per l'economia europea si trasformasse in uno strumento per eludere l'applicazione delle norme in materia di protezione dei dati o del diritto nazionale, il Regolamento 1807 ha stabilito il principio secondo cui l'accesso ai dati da parte delle autorità competenti non può essere rifiutato a motivo del loro trattamento in un altro Stato membro, mantenendo così inalterata la facoltà di chiedere e ottenere l'accesso per verificare che le caratteristiche dei dati coinvolti siano conformi alla legge. Oltre a ciò, l'accessibilità degli organi preposti alla vigilanza è favorita sia

[158] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Costruire un'economia dei dati europea* (COM (2017) 9 final), p. 2; Commissione europea, *Commission staff working document on the free flow of data and emerging issues of the European data economy. Accompanying the document "Communication Building a European data economy"* (SWD (2017) 2 final), p. 8; *"Cross-border data flow in the digital single market: study on data location restrictions"*, FINAL REPORT. *A study prepared for the European Commission DG Communications Networks, Content & Technology by: Time.lex, Spark Legal Network and Tech4i2* (SMART 2015/0054).

[159] Per il profilo della tutela dell'ordinamento costituzionale italiano si veda, SALERNO G. M., *Le garanzie della democrazia*, in *Rivista Associazione Italiana dei Costituzionalisti* n°: 3/2018.

[160] Commission staff working document impact assessment, Accompanying the document "Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union" (SWD (2017) 304 final, part 1/2).

dalle sanzioni che gli stessi possono imporre in caso di rifiuto ingiustificato – fra cui è stata aggiunta la rilocalizzazione dei dati – ,[161] sia dalla procedura di cooperazione tra autorità disciplinata dall'articolo 7.

Infine, il terzo ed ultimo profilo toccato dalla nuova disciplina riguarda la portabilità dei dati non personali per gli utenti professionali. Come verrà più dettagliatamente esposto nel prosieguo, colpiscono innanzitutto le significative differenze tra la portabilità dell'articolo 6 del RDNP e quella dell'articolo 20 del GDPR.[162] Diversi sono sia i beneficiari di tale istituto,[163] sia la posizione giuridica da essi ricoperta. Mentre alla persona fisica contemplata dal GDPR viene riconosciuto un vero e proprio diritto, l'utente professionale del RDNP può fare affidamento solamente sulle informazioni dettagliate e sui requisiti operativi per la portabilità, i quali "dovrebbero essere definiti dagli operatori del mercato mediante autoregolamentazione, incoraggiati, agevolati e controllati dalla Commissione, in forma di codici di condotta dell'Unione che potrebbero contemplare clausole e condizioni contrattuali tipo".[164] Questo approccio di autoregolamentazione è stato oggetto di severe critiche, poiché, così facendo, si tenta di raggiungere il medesimo scopo, consistente nella limitazione delle

[161] Regolamento (UE) 2018/1807, art. 5, par. 4.
[162] Differenza che nelle versioni francesi dei documenti è ben più evidente rispetto al caso italiano, poiché vengono impiegati termini distinti, rispettivamente "portage" e "portabilité". A tal proposito si veda, Parere del Comitato economico e sociale europeo (CESE) sulla "Comunicazione della Commissione al Parlamento europeo e al Consiglio - Linee guida sul regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea" adottato il 25 settembre 2019, p. 5.
[163] Il Regolamento 1807 non concerne il rapporto tra *data subject* e titolare del trattamento, ma rimane circoscritto all'ambito B2B, in quanto si rivolge a quei soggetti che, nel contesto della propria attività professionale, decidono di cambiare il fornitore di un determinato servizio.
[164] Regolamento (UE) 2018/1807, cons. n. 30.

pratiche di "vendor lock-in",[165] seguendo due strade differenti: la regolamentazione rigida per i dati personali e l'autodisciplina per i non personali, con il rischio di aumentare un'incertezza giuridica che, come spesso accade nella *data economy*, tende ad andare a discapito delle piccole e medie imprese.[166]

In conclusione, l'analisi storica svolta nella parte prima di questo capitolo consente di comprendere in maniera più adeguata le ragioni della strutturazione dell'ordinamento giuridico attualmente vigente. Tale assetto rappresenta il frutto sia di fattori inerenti alla cronistoria europea del XX secolo, sia di una precisa volontà di distinzione rispetto alle esperienze giuridiche di altri Paesi, specie quella statunitense. La sua genesi e la sua formazione sono state plasmate dalla forza centripeta che ha esercitato la fattispecie dei dati personali sul legislatore, sulla giurisprudenza e sulla dottrina degli Stati membri della Comunità, prima, e dell'Unione europea, poi. Il sentiero tracciato dal tribunale costituzionale tedesco nel 1983 e la coeva spinta delle organizzazioni internazionali hanno permesso di consolidare un sistema di norme che tutelasse l'individuo con un livello crescente di protezione, giacché le lesioni alla sfera giuridica personale e alla capacità di autodeterminazione patite da quest'ultimo erano riconducibili allo stretto legame che lo collegava ai suoi dati personali. Pertanto, malgrado il costante affiancamento della dimensione economica dei dati – segnatamente, del loro libero flusso – la caratterizzazione della disciplina come primariamente votata alla protezione di un diritto di rango fondamentale e, come

[165] La Commissione europea, nella *Guidance, op. cit.*, p. 18, afferma che: "queste pratiche si verificano quando gli utenti non possono cambiare il fornitore di servizi, perché i loro dati sono "bloccati" nel sistema del fornitore, ad esempio a causa di uno specifico formato dei dati o di accordi contrattuali, e non possono essere trasferiti al di fuori del suo sistema informatico".
[166] Parere del CESE adottato il 25 settembre 2019, *op. cit.*, p. 9.

visto, costituzionale ha catturato l'attenzione delle istituzioni europee. Del resto, le stesse direttive degli anni Novanta e Duemila testimoniano questa irrefrenabile tendenza all'istaurazione di un meccanismo di tutela individuale, ad onta della base giuridica e della vocazione economica della Comunità di quell'epoca. Con la proclamazione della Carta e il susseguente impulso giurisprudenziale teso a qualificare tale tutela come diritto fondamentale, l'Unione europea è finalmente uscita allo scoperto e ha rivelato l'impronta distintiva e originale del suo impianto normativo. L'attenzione di cui ha conseguentemente beneficiato l'individuo con riguardo alla protezione della sua sfera privata e, di riverbero, i suoi dati ha inevitabilmente restituito un ordinamento "dato personale-centrico" che non bilancia il dettaglio e la profondità delle regole poste a tutela della persona fisica con un altrettanto valido sistema regolamentare per le informazioni sprovviste del carattere personale. Se tale prospettiva poteva apparire condivisibile nell'epoca precedente, i moderni modelli di raccolta ed elaborazione di dati, che non risparmiano nessun tipo di informazione dal circuito di analisi, mettono fortemente in crisi l'impianto regolatorio continentale.

In ogni caso, la disciplina che il legislatore europeo ha predisposto per la fattispecie del dato non personale ha definitivamente certificato il doppio binario su cui si fonda il sistema europeo di regolamentazione di dati. Il GDPR e il Regolamento 1807, malgrado non abbiano – e non possano del resto avere – il medesimo rilievo, attestano per l'ennesima volta la peculiare considerazione che il legislatore unionale conserva nei confronti della realtà digitale. Nel capitolo successivo, si tenterà di illustrare quali ripercussioni possono avere due regimi distinti, che si richiamano vicendevolmente e che, nonostante tutto, sono messi in crisi dall'evoluzione tecnologica, sulla fondamentale dimensione della

libera circolazione dei dati all'interno ed all'esterno dell'Unione europea.

CAPITOLO II

LA LIBERA CIRCOLAZIONE DEI DATI TRA IL REGOLAMENTO (UE) 2016/679 E IL REGOLAMENTO (UE) 2018/1807

Sommario: 1. La circolazione dei dati come terreno di confronto. 2. L'Unione tra mercato dei dati europeo e *data localization* 3. La circolazione dei dati personali. 3.1 All'interno dell'Unione europea. 3.2 Al di fuori dell'Unione europea. 4. La circolazione dei dati non personali. 4.1 Il divieto degli obblighi di localizzazione. 4.2 Una nuova portabilità autoregolamentata: dalla "*portability*" al "*porting*". 5. Tessere mancanti nel mosaico regolamentare europeo?

1. La circolazione dei dati come terreno di confronto

L'esame in ottica comparativa dei due regolamenti generali attualmente vigenti in Europa in materia di dati verrà impostato adottando la libera circolazione delle informazioni quale terreno di confronto, al preciso scopo di intercettare le differenze che contraddistinguono le due normative e di comprendere quali conseguenze potrebbero derivare dalla biforcazione fissata dal legislatore continentale. Tale scelta di carattere metodologico è essenzialmente dettata da un duplice ordine di ragioni. Innanzitutto, le modalità di disciplina del flusso dei dati all'interno ed all'esterno dei confini dell'Unione europea rappresentano il minimo comun denominatore più solido per impostare un paragone valido tra le due normative. È chiaro che esaminare le norme solamente attraverso la lente della tutela dei diritti garantiti dai due atti significherebbe

strutturare l'analisi sulla base di una premessa capziosa ed ondivaga. Il regolamento relativo ai dati non personali non sarebbe, naturalmente, in grado di reggere una comparazione di tale tipo, giacché, a differenza del suo omologo, non prende in considerazione, se non in maniera meramente indiretta, la dimensione della tutela dei soggetti interessati dalle sue norme.

In secondo luogo, il tema della circolazione delle informazioni assume particolare rilievo nell'ambito della presente tesi in quanto dimensione cruciale della sovranità digitale e della *data dependance*.[1] Il fenomeno della *data driven innovation* è diventato l'indiscusso protagonista dell'attuale realtà economica e sociale nel giro di pochissimi anni, trasformandosi nel punto di riferimento per qualsiasi modello di sviluppo economico e tecnologico. Attualmente, il vero potere si trova nelle mani di chi, tramite la gestione di una vastissima mole di dati, riesce ad estrarre valore e, conseguentemente, prendere decisioni economicamente molto vantaggiose, a fronte di costi assai ridotti.[2]

L'importanza progressivamente assunta dai dati, i quali oggi, di fatto, si presentano come una risorsa economico-finanziaria di cui nessuna attività, né pubblica, né privata, può più fare a meno,[3] è riconducibile, oltre che agli imprevedibili e preziosi significati che possono essere estrapolati per mezzo dell'analisi di tali informazioni, anche alla loro inaudita capacità di circolazione che permette di prescindere dagli ostacoli naturali o artificiali che generalmente rallentano il trasferimento transfrontaliero dei beni. Pertanto, uno

[1] CALZOLAIO S., *Introduzione. Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati*, in *Rivista italiana di informatica e diritto*, fasc. n. 1/2021, pp. 7-11.
[2] OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being*, OCSE Publishing, Parigi, 2015.
[3] MCAFEE A., BRYNJOLFSSON E., *Big data: the management revolution*, in *Harvard Business Review*, n. 10/2012.

degli aspetti più importanti concernenti l'innovazione digitale è quello relativo al flusso di queste informazioni: l'addestramento degli algoritmi, le analisi di mercato, l'elaborazione di strategie pubbliche, l'adozione di piani aziendali sono tutte attività accomunate dalla stretta correlazione con il trattamento di una serie di dati che provengono da fonti diverse e, nella maggior parte dei casi, da Paesi diversi. In tal senso, dunque, la tematica del flusso di dati gioca un ruolo chiave in una realtà economico-giuridica che si contraddistingue per la sua globalità e per la rilevante presenza di catene di valore transfrontaliere.[4]

L'osservazione delle modalità per mezzo delle quali il legislatore europeo ha deciso di regolamentare il flusso di informazioni prodotte sul suolo continentale permette di maturare una precisa cognizione della categorizzazione che divide il mondo dei dati europeo. L'assetto ordinamentale, infatti, si basa sulla fondamentale distinzione tra dato personale e dato non personale e si sviluppa in due normative distinte che, malgrado comunicanti, rischiano di scostarsi troppo da una realtà digitale in cui tale distinzione è molto meno chiara di quanto la normativa lasci presupporre.[5]

2. L'Unione tra mercato dei dati europeo e *data localization*

Lo studio della circolazione quale fattore essenziale dell'economia contemporanea non può prescindere dall'esame del suo antagonista, gli obblighi di localizzazione, fenomeno

[4] ÜNVER H. A., KIM G., *Cross-Border Data Transfers and Data Localization*, EDAM Cyber Policy Paper Series 2016/3, pp. 2-6.
[5] MONTAGNANI M.L., *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in *Mercato concorrenza regole*, a. XXI, n. 2, agosto 2019, pp. 311-313.

internazionalmente conosciuto con il nome di "*data localization*". Il numero di tali obblighi è cresciuto parallelamente all'aumento dell'importanza dei dati per la società,[6] giacché anche il dato risponde all'antica logica secondo cui più un bene ha valore, più è incline al rischio di offesa e, di conseguenza, richiede maggiore tutela. Difatti, le principali ragioni che sono alla base dell'introduzione di misure legislative o amministrative da parte degli Stati a difesa del proprio patrimonio informativo riguardano la sicurezza interna, la facilità di accesso delle autorità nazionali alle informazioni necessarie alla vigilanza e, infine, lo sviluppo industriale domestico.[7]

Di regola, con il termine *data localization* non ci si riferisce solo ed esclusivamente a quelle misure che impongono, direttamente o indirettamente, il luogo in cui deve essere effettuato un determinato trattamento, poiché vengono ricomprese anche quelle disposizioni che fissano condizioni più o meno stringenti al trasferimento dei dati al di là dei confini nazionali.[8] Questa circostanza allarga enormemente il novero delle misure che possono rientrare nella definizione, coprendo sostanzialmente tutti gli ordinamenti che hanno una disciplina in materia di circolazione dei dati, in quanto, quando non impongono un divieto generale oppure permettono il trasferimento solo dopo un primo trattamento a livello locale,[9] si

[6] BAUER M., LEE-MAKIYAMA H., VAN DER MAREL E., VERSCHELDE B., *The Cost of Data Localisation: Friendly Fire on Economic Recovery*, ECIPE Occasional Paper No. 3/2014, pp. 3-10.
[7] FERRACANE M. F., *Restrictions on Cross-Border data flows: a taxonomy*, ECIPE Working Paper No. 1/2017, p. 6.
[8] FERRACANE, *Restrictions on Cross-Border data flows: a taxonomy*, *op. cit.*, pp. 2-3.
[9] Come, ad esempio, accade in Russia. Per un approfondimento, si veda: SAVELYEV A., *Russia's new personal data localization regulations: A step forward or a self-imposed sanction?*, in *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 2015.

premurano comunque di prescrivere una serie di condizioni affinché i dati possano abbandonare il territorio di provenienza.

Alla luce di queste considerazioni, le restrizioni alla libera circolazione possono distinguersi in "rigide" o "condizionali".[10] Le prime, quelle che obbligano il titolare ad eseguire una determinata fase del trattamento localmente, si suddividono a loro volta in sottocategorie, a seconda del rigore della misura: partendo da una disposizione che richiede il solo *storage* a livello locale – ossia mantenere una copia interna – e passando per quelle che, oltre all'archiviazione, impongono il *processing* domestico, si arriva fino al divieto generale di trasferimento, con la conseguenza che, al di fuori dei propri confini, è vietato persino il semplice accesso alle informazioni.[11] Le restrizioni condizionali, invece, lasciano sempre uno spazio, più o meno angusto, al trasferimento, ma lo rendono più gravoso nella misura in cui pretendono l'osservanza di alcuni requisiti da parte del soggetto trasferente o del ricevente, oppure di entrambi.[12] Tale distinzione si riflette anche sul bersaglio delle restrizioni: mentre quelle condizionali sono concepite al fine di limitare i trasferimenti di un determinato tipo di dato – generalmente personale –, quelle rigide hanno una dimensione prettamente settoriale, con la conseguenza che la distinzione tra dato personale e non personale non acquisisce alcuna rilevanza.[13]

A dispetto dell'incremento massivo, la dottrina è sostanzialmente concorde nel ritenere che gli effetti che la *data*

[10] FERRACANE M. F., *Restrictions on Cross-Border data flows: a taxonomy*, *op. cit.*, pp. 2-3.
[11] *Ibid.*, pp. 2-3.
[12] *Ibid*. Naturalmente, la realtà dei fatti non rispecchia così nettamente la classificazione appena svolta, giacché le differenze possono essere molto più labili di quanto si pensi, e anche una misura condizionale può facilmente tramutarsi in rigida se l'iter necessario ad addivenire al trasferimento è troppo oneroso per la dimensione in cui opera il trasferente.
[13] *Ibid.*, pp. 8-9.

localization produce nei confronti delle economie statali sono pressoché tutti negativi e che gli obiettivi di sicurezza, controllo e *privacy* che sono alla base dell'introduzione di simili misure restrittive potrebbero essere raggiunti tramite strade alternative che, oltre ad aiutare gli operatori del mercato, sarebbero in grado di apportare incalcolabili benefici al settore produttivo domestico.[14] Lo stesso discorso vale per un'organizzazione internazionale quale l'Unione europea che, dal canto suo, non è stata risparmiata da questa ondata di protezionismo che ha reso la *data localization* il principale attore non protagonista delle normative concernenti la gestione dei dati. Invero, più di uno studio sulle normative dei singoli Stati membri dell'Unione ha dimostrato che, anche nel nostro continente, l'aumento del valore dell'informazione è stato accompagnato da un clima di sfiducia nelle normative e, soprattutto, nei sistemi di sicurezza degli altri Paesi membri, sfociando in poco tempo nell'emanazione di una serie di obblighi giuridici atti ad internalizzare il trattamento nella misura più ampia possibile.[15]

Resosi conto di questa preoccupante tendenza, con l'inizio della seconda decade di questo secolo, il legislatore europeo ha deciso di prendere una posizione netta al riguardo, invertendo la rotta nel tentativo di smantellare le mura virtuali che dividevano gli Stati membri. Con queste premesse nasce la strategia per la creazione del "Mercato Unico Digitale", concepito nelle intenzioni delle istituzioni europee come un passo imprescindibile affinché il mercato interno

[14] BAUER M., LEE-MAKIYAMA H., VAN DER MAREL E., VERSCHELDE B., *The Cost of Data Localisation*, *op. cit.*, pp. 5-10.

[15] RYAN P.S., FALVEY S., MERCHANT R., *When the Cloud Goes Local: The Global Problem with Data Localization*, in *Computer*, Vol. 46, No. 12, 2013, pp. 54-59; CHANDER A., LE U. P., *Breaking the Web: Data Localization vs. the Global Internet*, Working Paper 2014-1, in *California International Law Center*, 2014, pp. 10-16; *"Cross-border data flow in the digital single market: study on data location restrictions"*, FINAL REPORT. *A study prepared for the European Commission DG Communications Networks, Content & Technology by: Time.lex, Spark Legal Network and Tech4i2* (SMART 2015/0054).

europeo possa continuare a funzionare nell'era della digitalizzazione.[16] Oggi è, difatti, impossibile condurre un'attività economica con caratteri transfrontalieri senza far fronte a tutte le questioni connesse al tema del trasferimento delle informazioni: i dati devono necessariamente muoversi assieme al bene al quale ineriscono, pertanto, in un mercato in cui gli ostacoli allo spostamento di persone, merci, capitali e servizi sono stati abbattuti, è chiaro che l'incentivo alla libera circolazione delle informazioni si manifesta come un passaggio irrinunciabile.[17]

Tra l'altro, riuscire nell'intento di trasformare simili iniziative in disposizioni normative efficaci e innovative rappresenta uno dei pochi ambiti in cui il vecchio continente può ancora imporsi quale capofila: se l'arretratezza tecnologica nei confronti dei giganti del *tech* che hanno le loro sedi nel Nord America e nell'Asia orientale non sembra potersi recuperare nel breve termine,[18] agire per rendere il mercato continentale più appetibile rimane un dovere dell'Unione europea.[19] Segnatamente, i primi passi mossi dagli organismi unionali verso l'abbattimento delle barriere virtuali alla libera circolazione, in favore di un incremento nell'utilizzo transfrontaliero

[16] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Strategia per il mercato unico digitale in Europa, (COM (2015) 192 final), pp. 15-21.

[17] La relatrice del Parlamento europeo Anna Maria Corazza Bildt, a seguito dell'approvazione del Regolamento (UE) 2018/1807, ha affermato che è stata introdotta una "quinta libertà di circolazione" che riguarda tutti i dati, https://www.europarl.europa.eu/news/en/press-room/20180926IPR14403/free-flow-of-non-personal-data-parliament-approves-eu-s-fifth-freedom.

[18] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale, (COM (2017) 228 final), pp. 23-26.

[19] BAUER M., LEE-MAKIYAMA H., VAN DER MAREL E., VERSCHELDE B., *The Cost of Data Localisation*, *op. cit*., pp. 12-13. In particolare: "a ban on data localisation is a powerful political message that the Single Market is open for business. This argument is particularly pertinent as the EU seeks to convince the market and turn the tide on the digital investments, and both inward and domestic investments into Europe's digital economy are withheld or diverted to other regions".

delle informazioni, risalgono al 2011, quando la Commissione europea riconosce che le precedenti normative in materia di armonizzazione e di incentivo all'apertura nell'utilizzo dei dati nel settore pubblico – in particolare la Direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico – non hanno sortito gli effetti sperati e che, di fatto, le barriere allo scambio di informazioni pubbliche costituiscono ancora un peso per l'economia continentale.[20] Tuttavia, dati i tempi non ancora maturi per una discussione profonda come quella odierna, soprattutto per quanto riguarda la distinzione tra dato personale e non personale, il documento circoscrive i suoi riferimenti ai dati pubblici, salvo qualche sporadico accenno alla tutela della vita privata e alla protezione dei dati personali.[21]

Dopo un'ulteriore comunicazione del luglio 2014 in cui viene evidenziato il problema degli ostacoli alla libera circolazione dei dati ed il loro effetto frenante nei confronti dello sviluppo del *cloud computing* e dello sfruttamento dei *Big Data*,[22] i documenti istituzionali del biennio 2017-2018 si focalizzano quasi esclusivamente sugli sforzi necessari alla creazione del mercato unico digitale. Secondo la visione europea, lo sviluppo di tutte le tecnologie basate sullo scambio di informazioni – dal *cloud*

[20] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Dati aperti Un motore per l'innovazione, la crescita e una governance trasparente (COM(2011) 882 final), pp. 7-8. In particolare: "Nonostante l'armonizzazione minima introdotta dalla direttiva del 2003 sul riutilizzo delle informazioni del settore pubblico, permangono differenze significative nelle norme e pratiche nazionali, con conseguente frammentazione del mercato interno dell'informazione e presenza di ostacoli alla creazione di servizi di informazione transfrontalieri".

[21] Comunicazione della Commissione, Dati aperti Un motore per l'innovazione, la crescita e una governance trasparente, *op. cit.*, pp. 5-6.

[22] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Verso una florida economia basata sui dati, (COM(2014) 442 final), pp. 12-13.

computing, all'*Internet of Things*, dalla *data analysis*, all'intelligenza artificiale – sono in grado di crescere e prosperare all'interno dell'economia continentale grazie a due pilastri fondamentali. Da un lato, la protezione dei dati personali, la quale, una volta aggiornata e consolidatasi nell'ordinamento europeo a tutti i livelli, promette di mantenere l'essere umano come centro gravitazionale attorno al quale si sviluppa la tecnologia, e non viceversa. Dall'altro lato, invece, si trova la libera circolazione dei dati, sia personali che non, la quale, accompagnata da una (non ancora del tutto) aggiornata disciplina riguardante l'interoperabilità e l'accesso alle informazioni, costituirà un incentivo senza eguali al progresso dell'economia europea.

Tuttavia, come anticipato, ciò che distingue sin da subito l'ordinamento europeo dai regimi giuridici dei Paesi tecnologicamente più avanzati, è proprio la preponderanza che il primo dei due pilastri, la protezione dei dati personali, assume nei confronti della libera circolazione delle informazioni. Prendendo come termine di paragone due fra i Paesi *leader* dell'attuale panorama mondiale, negli Stati Uniti la disciplina riguardante le informazioni relative alle persone fisiche viene ancora percepita in un'ottica perlopiù consumeristica, con la conseguenza che l'individuo riesce ad ottenere protezione proprio in quanto consumatore, ma non in quanto persona che gode di un diritto fondamentale alla protezione dei propri dati.[23] Una impostazione altrettanto differente è invece quella riguardante la Repubblica popolare cinese, dove, in un certo senso, traspare una duplice concezione: se, per un verso, l'ordinamento cinese sembra si stia avvicinando a quello europeo nell'ambito delle relazioni fra privati,

[23] MIGLIETTI L., *Profili storico-comparativi del diritto alla privacy*, in *diritticomparati.it*, 2014, pp. 8-13.

per altro verso, il precedente approccio centralizzato continua a caratterizzare la disciplina nei rapporti verticali fra individuo e governo, secondo un sistema autoritario e gerarchico che pone al vertice la sicurezza dello Stato.[24]

Nell'Unione europea, invece, proprio la circostanza che la posizione centrale della disciplina giuridica sia ricoperta dalla persona fisica e dai suoi diritti fondamentali rappresenta il principale motivo per cui l'impianto normativo dedicato alle altre dimensioni del *data law*, soprattutto, quella economica, si sia sviluppato in un secondo momento o, quantomeno, sia stato ipotizzato come sussidiario. Infatti, è dopo l'approvazione del GDPR, precisamente nella Comunicazione sulla costruzione di un'economia dei dati europea del 2017, che è stata concepita l'idea di un regolamento specificamente dedicato ai dati a carattere non personale. [25] Effettivamente, dal testo emerge la ormai raggiunta consapevolezza che per lo sviluppo di un'economia sana e stabile non è sufficiente la sola tutela dell'individuo, poiché si rivela fondamentale anche mettere le imprese e le pubbliche amministrazioni in una posizione che dia loro la possibilità di essere promotrici di un nuovo modello economico-sociale.[26] Pertanto, la Commissione sottolinea quanto sia importante un approccio organico alla materia e chiarisce espressamente che il principio della libera circolazione dei dati all'interno dell'Unione, inteso quale corollario imprescindibile delle altre libertà riconosciute nel mercato unico europeo, non riguarda

[24] Per un approfondimento, si vedano: DE HERT P., PAPAKONSTANTINOU V., *The data protection regime in China*, *In-depth Analysis for the LIBE Committee*, 2015, pp. 13-27; YUEXIN Z., *Cyber protection of personal information in a multi-layered system*, in *Tsinghua China Law Review*, n. 2/2019.
[25] COLPAERT C., JANSSENS M-C., *Work in progress: the proposal of the free flow of non-personal data regulation*, in *CITIP Blog*, 2018.
[26] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, "Costruire un'economia dei dati europea", (COM(2017) 9 final), pp. 9-14.

solo i dati personali – come avviene nel GDPR – ma interessa tutte le tipologie di informazioni.[27] Tuttavia, subito dopo questa statuizione che potremmo definire pionieristica, interviene una ulteriore precisazione volta a rimarcare la differenza insita in quei regimi giuridici dei dati che attuano il medesimo principio di libera circolazione: mentre le norme concernenti il flusso dei dati possono essere il risultato di trattative con Paesi terzi, quelle relative alla protezione dei dati personali hanno uno status diverso, in quanto, godendo del rango di diritto fondamentale, non possono essere oggetto di negoziazione.[28]

Un ulteriore documento finalizzato alla costruzione delle fondamenta del mercato unico digitale, in cui l'eterogeneità del regime giuridico europeo in materia di circolazione dei dati si avverte con maggiore evidenza, è la Comunicazione "Verso uno spazio europeo comune dei dati". In tal caso, lo scopo principale della Commissione risiede nella proposizione del cosiddetto "*data package*", ossia di un insieme di tre provvedimenti che, in aggiunta alla normativa sulla protezione dei dati personali e al regolamento sulla circolazione dei dati non personali – all'epoca non ancora definitivamente approvato –, mira a creare "uno spazio comune dei dati nell'UE, un'area digitale senza soluzione di continuità, la cui scala consenta lo sviluppo di nuovi prodotti e servizi basati sui dati".[29]

La proposta della Commissione sfocia nell'adozione di tre documenti diversi che, nonostante non si traducano tutti in strumenti di *hard law*, di fatto predispongono o incentivano la creazione di

[27] *Ibid.*, pp. 2-5.
[28] *Ibid.*
[29] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, "Verso uno spazio comune europeo dei dati", (COM(2018) 232 final), p. 1.

regole differenti per i dati a seconda del settore in cui essi vengono trattati.[30] Se il primo strumento, ossia la direttiva relativa al riutilizzo dell'informazione nel settore pubblico, fa riferimento ad un ampliamento della politica di messa a disposizione dei dati definiti come "pubblici",[31] il secondo consiste in una Raccomandazione volta ad incentivare il regime di *open access* per i dati raccolti e trattati nell'ambito della ricerca scientifica.[32] Il terzo provvedimento, infine, riguarda gli orientamenti sulla condivisione dei dati nel settore privato, tramite i quali la Commissione si offre quale promotrice di principi, accordi e regole a cui gli operatori privati dovrebbero fare ricorso al fine di trasformare il mercato europeo in un grande *hub* di informazioni, da cui tutti potrebbero trarre beneficio.[33] Ciò che accomuna i tre provvedimenti è l'idea di una politica, o meglio, di una cultura di condivisione dei dati che non si limiti semplicemente al settore pubblico – già in parte destinatario di un'apposita direttiva – ma che riguardi anche il settore privato nei rapporti tra imprese e nei rapporti tra imprese ed enti pubblici.

Peraltro, nonostante l'intenzione fosse quella di incentivare lo spostamento delle informazioni all'interno del territorio continentale nella misura più ampia possibile, è evidente che la vasta gamma di strumenti regolatori messi in campo dalle istituzioni europee rischia di tradursi in una settorializzazione e stratificazione normativa in grado di compromettere la libera circolazione.[34]

---

[30] MONTAGNANI M.L., *La libera circolazione dei dati al bivio*, *op. cit.*, pp. 298-302.
[31] Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.
[32] Raccomandazione (UE) 2018/790 della Commissione del 25 aprile 2018 sull'accesso all'informazione scientifica e sulla sua conservazione.
[33] Documento di lavoro dei servizi della Commissione, Orientamenti sulla condivisione dei dati del settore privato nell'economia europea dei dati che accompagna il documento Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "Verso uno spazio comune europeo dei dati" (SWD(2018)125 final).
[34] MONTAGNANI M.L., *La libera circolazione dei dati al bivio*, *op. cit.*, pp. 298-302.

3. La circolazione dei dati personali

3.1 All'interno dell'Unione europea

La concezione della protezione dell'individuo con riferimento al trattamento delle sue informazioni come diritto di rango fondamentale ha ingenerato un impianto normativo progettato al preciso scopo di ancorare la tutela giuridica continentale all'informazione, continuando a seguirla in ogni suo spostamento, come una garanzia che non può essere scissa dal bene al quale si accompagna.[35] Questo principio pervade l'intera normativa e, infatti, ha rappresentato uno dei capisaldi attorno ai quali è stata modellata la nuova disciplina in materia di circolazione dei dati personali, sia dal punto di vista interno, ossia limitato al flusso intra-europeo, sia dal punto di vista esterno, quando i dati lasciano l'Unione.

Per quanto riguarda la circolazione tra gli Stati membri, con l'impiego della fonte regolamentare in luogo della precedente direttiva, il legislatore europeo è riuscito ad uniformare le discipline nazionali, cosicché, almeno teoricamente, ogni regime giuridico conforme al GDPR deve assicurare lo stesso livello di tutela.[36] Pertanto, alla luce della forte spinta verso l'armonizzazione in

[35] KIRSCHEN S., *Il trasferimento all'estero dei dati*, in PANETTA (a cura di), *Circolazione e protezione dei dati personali tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, 2019, pp. 265-268.

[36] Regolamento (UE) 2016/679, considerando n. 13. In particolare: "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, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri. Per il buon funzionamento del mercato interno è necessario che la libera circolazione dei dati personali all'interno dell'Unione non sia limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali".

materia di protezione dei dati, l'articolo 1, paragrafo 3 del GDPR stabilisce che i singoli Stati membri non possono più lamentare una lacuna nella protezione di tali dati come motivo alla base dell'imposizione di un divieto di trasferimento al di fuori dei propri confini.[37] Invero, nonostante anche la precedente direttiva esordisse con parole simili, la mancata armonizzazione dovuta all'impiego di una fonte normativa "più debole" non era di fatto riuscita a limitare la propagazione degli obblighi di localizzazione dettati da motivi attinenti alla tutela della *privacy* delle persone fisiche. Anzi, proprio gli ultimi anni di vigenza della direttiva sono stati testimoni di una proliferazione di restrizioni senza precedenti, non solo a causa dell'avvento della digitalizzazione, ma anche perché la promessa di un elevato livello di protezione dei dati veniva utilizzata come giustificazione di tali misure.[38]

Ad ogni modo, nonostante la libera circolazione non venga espressamente annoverata tra i principi fondamentali del GDPR, una chiara affermazione in tal senso proviene direttamente dalla Commissione europea la quale, nell'intento di allargarne l'applicazione anche ai casi in cui agli Stati membri è consentito disciplinare materie specifiche, afferma che questi "dovrebbero essere incoraggiati a non fare uso delle clausole di deroga del regolamento per limitare ulteriormente la libera circolazione dei dati".[39]

---

[37] Regolamento (UE) 2016/679, art. 1, par. 3: "La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali".

[38] BAUER M., FERRACANE M. F., LEE-MAKIYAMA H., VAN DER MAREL E., *Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States,* ECIPE Occasional Paper No. 3/2016, pp. 3-8.

[39] Comunicazione della Commissione, "Costruire un'economia dei dati europea", *op. cit.*, pp. 5-8.

Tuttavia, se il Regolamento generale sulla protezione dei dati personali rappresenta un apparato giuridico che, oltre che tutelare l'individuo, è funzionale al contrasto dell'insorgenza degli obblighi di *data localization*, è opportuno rammentare che i mezzi attraverso i quali gli Stati membri sono in grado di introdurre nuove restrizioni, o mantenere quelle già esistenti, non ricadono tutti nell'ambito di applicazione del GDPR.[40] Mentre la protezione della *privacy* degli individui non può più fungere da scudo della localizzazione, i singoli Paesi possono ancora fare affidamento sulle deroghe previste da altre fonti settoriali del diritto europeo riguardanti la gestione dei dati,[41] le quali, in ogni caso, dovranno comunque superare il vaglio relativo alla loro compatibilità con quanto stabilito dal diritto dell'Unione in materia di libertà fondamentali.[42]

A tal proposito, non ci si può esimere dal sottolineare ancora una volta come la moltitudine di fonti normative europee, nel tentativo di regolamentare dettagliatamente la gestione dei dati, non

[40] Nella Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union* (COM (2019) 250 final), p. 15, è riportato un esempio eloquente al riguardo: "Una normativa nazionale prevede che la contabilità del personale sia situata in uno specifico Stato membro per ragioni riguardanti il controllo regolamentare, ad es. da parte dell'amministrazione fiscale nazionale. Tale normativa nazionale non rientrerebbe nell'ambito di applicazione dell'articolo 1, paragrafo 3, del regolamento generale sulla protezione dei dati, in quanto i motivi non riguardano la protezione dei dati personali. Questo obbligo dovrebbe invece essere valutato sulla base delle disposizioni relative alle libertà fondamentali e delle deroghe consentite a tali libertà previste nel trattato sul funzionamento dell'Unione europea".

[41] A tale proposito, si rimanda, senza pretesa di esaustività, a: Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno; Direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno; Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione.

[42] Comunicazione della Commissione, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, *op. cit.*, pp. 14-15.

faccia altro che offrire ulteriori opportunità per l'introduzione di impedimenti al libero flusso delle informazioni.

3.2 Al di fuori dell'Unione europea

Un discorso diverso vale, invece, se si rivolge lo sguardo alle modalità con cui l'Unione europea disciplina la circolazione dei dati al di fuori dei propri confini, poiché è lo stesso ordinamento giuridico continentale a trasformarsi in un parziale obbligo di localizzazione dei dati personali.

Anche il meccanismo di trasferimento di informazioni personali verso Paesi terzi o organizzazioni internazionali, come altri istituti del regolamento, muove dalla precedente impostazione sancita dalla Direttiva 95/46/CE, riadattandola al nuovo contesto digitalizzato in cui si trova ad operare e, soprattutto, cristallizzando le regole di origine giurisprudenziale elaborate dalla Corte di giustizia dell'Unione.[43] Pertanto, affinché i dati personali possano lasciare il territorio europeo, gli articoli 44 e seguenti del GDPR predispongono una serie di condizioni in assenza delle quali il trasferimento non può avere luogo. Dunque, nonostante il legislatore abbia predisposto un ampio ventaglio di possibilità di trasferimento capaci di adeguarsi al tipo di situazione in cui versa il titolare del trattamento, stando alla definizione generale di *data localization*, anche l'ordinamento giuridico europeo rientra a pieno titolo nel novero di quelle misure atte a limitare la libera circolazione.[44]

Il ragionamento alla base del divieto di imporre obblighi di localizzazione all'interno dell'Unione, viene in questo caso

[43] A tale riguardo si rimanda alle decisioni illustrate nel primo capitolo, in particolare le sentenze *Google Spain SL* e *Schrems*.
[44] URBIOLA P., *Data Flows Across Borders. Overcoming Data Localization Restrictions*, Institute of International Finance, 2019.

impiegato *a contrario* proprio per condizionare il trasferimento verso l'esterno: dal momento in cui la tutela dei dati personali è ben lontana dal poter essere considerata omogenea a livello globale, l'Unione ha deciso di introdurre un meccanismo che sia in grado, quantomeno nelle intenzioni, di agganciare al dato la tutela continentale anche quando questo esce dall'ordinamento giuridico di origine.[45] Questa caratteristica peculiare garantisce una sorta di ultra-attività territoriale delle regole europee,[46] atteso che queste impongono il loro rispetto non solo la prima volta che i dati abbandonano l'Europa, ma anche per i trasferimenti successivi.[47]

Entrando nel dettaglio della disciplina, si nota sin da subito come il Regolamento generale racchiude una serie di regole in cui il flusso internazionale dei dati è percepito come un "elemento strutturale" [48] della normativa e non più, come accadeva nella Direttiva – in vigore in un momento storico in cui lo spostamento delle informazioni tra Stati non aveva la rilevanza che ha oggi – come circostanza episodica annoverabile fra le ipotesi delle mere eccezioni. Dunque, la disciplina che governa il meccanismo di trasferimento esordisce con il principio generale in ragione del quale i dati possono lasciare il territorio europeo solamente se rispettano le condizioni del capo V. Lungi dal prescrivere un divieto generale

[45] Comunicazione della Commissione, Scambio e protezione dei dati personali in un mondo globalizzato, (COM(2017) 7 final), pp. 4-6. In particolare: "L'obiettivo principale di tali norme è garantire che, quando i dati personali dei cittadini europei vengono trasferiti all'estero, la tutela viaggi con loro".
[46] ZENO-ZENCOVICH V., *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in RESTA, ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Collana "Consumatori e Mercato", 2016, pp. 7-21; VALLE L., GRECO L., *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale*, in *Il diritto dell'informazione e dell'informatica*, Anno XXXII, Fasc. 2-2017, pp. 198-201; KIRSCHEN S., *Il trasferimento all'estero dei dati*, *op. cit.*, p. 265-268.
[47] Regolamento (UE) 2016/679, art. 44.
[48] KIRSCHEN S., *Il trasferimento all'estero dei dati op. cit.*, p. 261-265.

come le misure restrittive più rigide, la consapevolezza raggiunta dal GDPR in merito alla essenzialità del flusso internazionale dei dati lo colloca nel complesso degli obblighi di localizzazione condizionali più tenui fra quelli attualmente in vigore.[49]

A conferma di ciò, è possibile constatare che se la decisione di adeguatezza, di cui all'articolo 45,[50] rimane il modello generale per il trasferimento come avveniva in precedenza,[51] ora questo stesso strumento viene potenziato poiché tanto il diritto europeo quanto quello nazionale non possono fissare limiti al trasferimento extra-europeo nei confronti di quei Paesi o organizzazioni internazionali il cui ordinamento giuridico è stato riconosciuto come adeguato.[52] Tale previsione si inserisce nel disegno generale promosso dal legislatore europeo verso quella che sembra essere una maggiore apertura del continente, con lo scopo di rafforzare le relazioni con altri Paesi, senza però sacrificare la tutela dell'individuo.[53]

---

[49] FERRACANE M. F., *Restrictions on Cross-Border data flows: a taxonomy*, *op. cit.*, p. 5.
[50] Regolamento (UE) 2016/679, art. 45, par.1: "Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche".
[51] KIRSCHEN S., *Il trasferimento all'estero dei dati*, *op. cit.*, p. 261-272; VALLE L., GRECO L., *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale*, *op. cit.*, pp. 188-191.
[52] Infatti, l'articolo 49, paragrafo 5 del GDPR recita: "In mancanza di una decisione di adeguatezza, il diritto dell'Unione o degli Stati membri può, per importanti motivi di interesse pubblico, fissare espressamente limiti al trasferimento di categorie specifiche di dati verso un paese terzo o un'organizzazione internazionale. Gli Stati membri notificano tali disposizioni alla Commissione". KIRSCHEN S., *Il trasferimento all'estero dei dati*, *op. cit.*, p. 283-291. Tuttavia, come visto con la sentenza *Schrems* e come confermato nella successiva *Schrems* II, una decisione di adeguatezza della Commissione europea può essere invalidata dalla Corte di giustizia.
[53] *Contra*: VALLE L., GRECO L., *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale*, *op. cit.* pp. 218-219. In particolare: "[…] per quanto concerne l'altro profilo della regolazione transfrontaliera dei dati personali relativo al trasferimento verso Paesi terzi esso è legato a dei canoni, come quello del controllo dell'adeguatezza della disciplina del Paese terzo e della decisione sull'adeguatezza di clausole standard da parte della Commissione europea, che poco si adattano ad un flusso di

Un ulteriore aggiornamento della disciplina concerne la nuova impostazione assunta dal GDPR in materia di deroghe. Se prima tutto ciò che ricadeva fuori dalla decisione di adeguatezza era classificato come deroga, oggi questa qualifica spetta solamente alle ipotesi specifiche – e più numerose rispetto al passato – [54] elencate nell'articolo 49.[55] Ciononostante, la predisposizione di un sistema derogatorio apparentemente a maglie più larghe, non si traduce in un lasciapassare volto ad eludere le disposizioni in materia di protezione di dati: il Comitato europeo per la protezione dei dati è intervenuto sul punto con delle apposite linee guida, insistendo sul fatto che l'interpretazione delle disposizioni all'articolo 49 deve essere la più restrittiva possibile.[56]

Infine, sulla base della stessa logica innovativa sono state aggiornate le garanzie adeguate, ossia quelle misure per mezzo delle quali è possibile trasferire i dati personali verso un Paese terzo il cui ordinamento giuridico non è stato valutato come adeguato da parte della Commissione europea. Il sistema in vigore, oltre a risultare più centralizzato rispetto al passato grazie ai maggiori poteri di controllo preventivo e autorizzatorio concessi agli attori istituzionali, dimostra ancora una volta la presa di coscienza da parte del Regolamento del fatto che il movimento dei dati da un continente all'altro sia diventato

dati quale quello che si reputa conveniente allo sviluppo delle attività economiche nel mondo contemporaneo".

[54] KIRSCHEN S., *Il trasferimento all'estero dei dati*, *op. cit.*, p. 283-291.

[55] L'elenco delle deroghe di cui all'articolo 49 del GDPR ricomprende: il consenso esplicito dell'interessato, l'esecuzione o la conclusione di un contratto in cui l'interessato è parte o beneficiario, importanti motivi di interesse pubblico, difesa o esercizio di un diritto in sede giudiziale, interessi vitali, quando le informazioni sono contenute in un registro aperto alla consultazione pubblica e, infine, interessi legittimi cogenti del titolare del trattamento.

[56] European Data Protection Board (EDPB), Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 2018. Invero, il Comitato, forzando il significato letterale del testo, afferma che i concetti di "occasionalità" e "non ripetitività" indicati con riferimento alla sola eccezione relativa agli interessi legittimi cogenti del titolare del trattamento, devono essere applicati a tutte le ipotesi previste nell'articolo, anche se non indicato esplicitamente.

un elemento essenziale dell'economia moderna. Il GDPR riesce a bilanciare la tutela dell'individuo con la circolazione dei dati personali tramite la responsabilizzazione dei soggetti coinvolti, ossia titolari e responsabili del trattamento, i quali, siano essi mittenti o riceventi, devono definire misure negoziali o paranegoziali al fine di sopperire alle lacune del sistema giuridico applicabile.[57] Oltre all'impiego di clausole contrattuali tipo, codici di condotta, meccanismi di certificazione o altri strumenti vincolanti, una delle principali novità risiede nell'introduzione delle "norme vincolanti d'impresa" (*Binding Corporate Rules*, o BCRs).[58] Mentre nel testo della Direttiva non erano affatto prese in considerazione,[59] queste disposizioni sono state concepite con l'intenzione di favorire lo scambio di informazioni sia nei gruppi imprenditoriali che nei "gruppi di imprese che svolgono un'attività comune"[60], di fatto prevenendo la formazione di barriere alla libera circolazione di informazioni che ostacolerebbero non poco l'attività commerciale del gruppo. L'inserimento delle BCRs e l'aggiunta di un articolo a sé stante nel regolamento segnano una presa di posizione forte da parte

[57] KIRSCHEN S., *Il trasferimento all'estero dei dati*, *op. cit.*, p. 274-283.

[58] L'articolo 4, punto 20, del GDPR definisce le norme vincolanti d'impresa come "le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune". Pertanto, tali norme sono costituite da quell'insieme di regole, politiche e strumenti applicabili (solamente) all'interno delle società del gruppo al fine di assicurare il rispetto dei principi, dei diritti e degli obblighi riguardanti la protezione dei dati personali nell'Unione europea. Per un approfondimento si veda, RICCIO G. M., *Model Contract Clauses e Corporate Binding Rules: valide alternative al Safe Harbor Agreement?*, in RESTA, ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Collana "Consumatori e Mercato", 2016.

[59] Tuttavia, il loro impiego non era sconosciuto prima dell'avvento del GDPR, tanto che il Gruppo di lavoro Articolo 29 si era già espresso a tale riguardo nel 2003: Article 29 Data Protection Working Party (WP29), "*Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*" (WP74).

[60] KIRSCHEN S., *Il trasferimento all'estero dei dati*, *op. cit.*, p. 274-283.

dell'Unione europea poiché, dalla totale assenza nella normativa precedente, sono ora divenute un *unicum* nel panorama del trasferimento extra-europeo dei dati personali, differente da tutte le altre garanzie. [61]

Ad ogni modo, il fatto che l'ordinamento giuridico europeo risulti essere una normativa moderna, attenta alle esigenze delle imprese che conducono attività a carattere transfrontaliero e a maglie più larghe rispetto ad altri sistemi giuridici, non è sufficiente, come detto, a precluderne la qualificazione di regime giuridico di *data localization*. [62] Oltretutto, questa situazione sembra destinata a permanere ancora a lungo, giacché, se la motivazione alla base di questa restrizione risiede nella tutela della *privacy* degli individui che in altri ordinamenti potrebbe risultare non adeguatamente salvaguardata, l'eventuale soppressione delle condizioni restrittive presupporrebbe il raggiungimento di un livello di armonizzazione globale che, ad oggi, sembra lontano. [63] Invero, dal momento che numerosi Paesi stanno virando verso un'impostazione giuridica in materia di tutela di dati e di localizzazione degli stessi non necessariamente simile a quella del vecchio continente, si può presumere che negli anni a venire, anziché ad una omogeneizzazione della normativa, assisteremo all'acuirsi dell'arroccamento all'interno delle proprie fortezze informatiche da parte di Stati gelosi del proprio patrimonio digitale e della sovranità che da esso dipende.

[61] *Ibid.*
[62] Per una visione critica (e metaforica) del meccanismo europeo, si veda: MANTELERO A., *From Safe Harbour to Privacy Shield. The "Medieval" sovereignity on pesonal data*, in *Contratto e Impresa/Europa*, 2016.
[63] FOCARELLI C., *La Privacy. Proteggere i dati personali oggi*, Bologna, 2015, pp. 123-175.

4. La circolazione dei dati non personali

Nella mente del legislatore europeo, il Regolamento relativo ad un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea nasce come strumento diretto a colmare le lacune emerse dopo l'approvazione del GDPR, il quale, circoscrivendo il suo ambito di applicazione alla categoria dei dati personali, aveva lasciato senza copertura altre tipologie di informazione ed i relativi obblighi di localizzazione.[64]

Per quanto concerne la dimensione della circolazione esterna all'Unione, è percepibile *ictu oculi* una profonda differenza intercorrente tra il Regolamento generale sui dati personali e il RDNP. Malgrado, contrariamente a quanto fatto dal GDPR, il RDNP sia principalmente focalizzato sul tema della circolazione e dell'accesso delle autorità amministrative in una dimensione prettamente interna, la sorte che spetta ai dati non personali – che sfuggono all'applicazione del meccanismo condizionale previsto dagli articoli 44 e seguenti del GDPR – nell'ipotesi in cui essi vengano destinati verso Paesi terzi non sembra essere stata presa in debita considerazione.[65] Pertanto, se da un lato, salvo l'unica eccezione relativa alla pubblica sicurezza che si vedrà in seguito, il regolamento non sembra contenere disposizioni di *data localization*, dall'altro, la mancanza di riferimenti alla dimensione extraeuropea potrebbe incoraggiare lo spostamento di informazioni di inestimabile

[64] Comunicazione della Commissione, "Costruire un'economia dei dati europea", *op. cit.*, pp. 5-8.

[65] Comunicazione della Commissione, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, op. cit.*, pp. 15-16. In particolare: "Il 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 non riguarda gli obblighi di localizzazione di dati imposti dagli Stati membri sull'archiviazione dei dati non personali in un paese terzo, che possono essere presenti negli ordinamenti giuridici nazionali".

valore per lo sviluppo delle nuove tecnologie in ordinamenti giuridici che rispondono a regole diverse, incentivando, pertanto, lo sfruttamento di questi dati solamente all'estero, dove l'Unione europea non potrebbe né controllarli né trarne alcun beneficio.[66]

Rivolgendo ora l'attenzione a quanto avviene all'interno del territorio continentale, è possibile osservare che il legislatore europeo ha deciso di incentivare la libera circolazione concentrando i propri sforzi, sia verso il settore pubblico, con l'abbattimento degli obblighi di localizzazione derivanti da legislazioni o pratiche amministrative in vigore negli Stati membri,[67] sia verso il settore privato, tramite l'incoraggiamento della portabilità delle medesime informazioni nell'ambito delle attività degli utenti professionali,[68] in maniera tale da prevenire le pratiche di *vendor lock-in* nemiche del mercato unico.[69]

4.1 Il divieto degli obblighi di localizzazione

Il primo scopo che il Regolamento 1807 intende perseguire è quello di eliminare le restrizioni ingiustificate alla libera circolazione dei dati non personali, considerate dalla Commissione europea il più grande ostacolo allo sviluppo dell'economia dei dati

[66] Parere del Comitato economico e sociale europeo (CESE) sulla «Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea» (2018/C 227/12), p. 6. In particolare: "Inoltre, la proposta della Commissione non tiene debito conto della natura globale e transeuropea dell'economia digitale e si preoccupa solo di regolamentare il mercato interno, dimenticando che quest'ultimo si sviluppa in un mercato globale, senza alcuna garanzia che gli altri paesi e continenti seguano le stesse regole che essa stessa intende attualmente applicare e senza il potere di imporle nei negoziati internazionali".
[67] Regolamento (UE) 2018/1807, cons. n. 4.
[68] La figura dell'"utente professionale" è definita dal punto 8, dell'articolo 3 del Regolamento come: "una persona fisica o giuridica, compreso un'autorità pubblica e un organismo di diritto pubblico, che utilizza o richiede servizi di trattamento di dati per fini connessi alla sua attività commerciale, industriale, artigianale, professionale o a una sua funzione".
[69] Regolamento (UE) 2018/1807, cons. n. 6.

nell'Unione.[70] In virtù di ciò, la norma centrale del regolamento è l'articolo 4, paragrafo 1, il quale vieta agli Stati membri l'introduzione e il mantenimento di obblighi di localizzazione dei dati quando non giustificati da motivi di pubblica sicurezza.[71] Ai fini del Regolamento, sono identificati quali obblighi di localizzazione le disposizioni di legge, gli orientamenti o le pratiche amministrative che, direttamente o indirettamente, impongono l'elaborazione o la conservazione dei dati limitatamente ad una determinata area geografica.[72] In particolare, i documenti degli organi europei fanno spesso riferimento alle richieste delle autorità di controllo di archiviare localmente i propri dati, alle regole del segreto professionale che prediligono il trattamento a livello locale, alle linee guida amministrative che dispongono lo stesso principio relativamente ai dati gestiti da enti pubblici e, non da ultimo, alle norme di settore che impongono l'utilizzo di dispositivi omologati in un determinato Stato membro.[73]

L'identificazione di simili restrizioni risulta molto più complessa di quanto possa apparire a prima vista. Uno studio di particolare interesse, eseguito anteriormente all'adozione definitiva del Regolamento, tende a distinguere tra due diverse categorie.[74] *In primis*, ci sono le cosiddette "barriere dirette", individuabili in

---

[70] Commissione europea, *Staff working document impact assessment, Accompanying the document "Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union"* (SWD (2017) 304 final, part 1/2).

[71] L'articolo 4, rubricato "Libera circolazione dei dati all'interno dell'Unione", al paragrafo 1 stabilisce: "Gli obblighi di localizzazione di dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità. Il primo comma del presente paragrafo fa salvo il paragrafo 3 e gli obblighi di localizzazione dei dati stabiliti sulla base del diritto vigente dell'Unione".

[72] Regolamento (UE) 2018/1807, art. 3, punto 5.

[73] Commissione europea, *Staff working document impact assessment, op. cit*.

[74] *"Cross-border data flow in the digital single market: study on data location restrictions"*, *op. cit.* Questo studio molto approfondito identifica gli obblighi di localizzazione che si possono trovare in alcuni Stati membri dell'Unione europea, p. 18.

maniera più agevole, le quali includono tutte le misure normative che stabiliscono espressamente dove conservare – o non conservare – i dati oppure che contengono obblighi tali per cui il loro rispetto può essere garantito solo tramite la conservazione in un determinato territorio.[75] Più ardue da riconoscere sono, invece, le "barriere indirette". Queste comprendono quelle norme la cui interpretazione può ragionevolmente limitare la scelta di chi gestisce i dati per quanto riguarda il luogo di archiviazione e il libero flusso.[76] In sostanza, le barriere indirette proliferano grazie a quelle prescrizioni che, senza arrivare a dettare un dovere di localizzazione vero e proprio, si inseriscono in un regime giuridico, o politico, nel contesto del quale la conservazione dei dati all'interno di un determinato territorio appare la soluzione interpretativa più opportuna.[77] .

[75] A titolo esemplificativo, possono essere citate due fra le più recenti barriere dirette introdotte dal legislatore italiano. La prima è contenuta nel d.l. 21 settembre 2019, n. 105, recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica" convertito con l. 18 novembre 2019, n. 133, il quale, tramite la creazione di un perimetro di sicurezza nazionale cibernetica, potrebbe limitare la circolazione di informazioni inerenti all'esercizio di "una funzione essenziale dello Stato" oppure alla "prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale". La seconda barriera, invece, può rinvenirsi nell'art. 6 del d.l. 30 aprile 2020, n. 28 convertito con l. 25 giugno 2020, n. 70, recante "Misure urgenti per l'introduzione del sistema di allerta Covid-19", che istituisce una piattaforma unica nazionale per la gestione del sistema di allerta degli utenti che usufruiscono della app "Immuni". Per un approfondimento, si rinvia a CALZOLAIO S., *Sistema di allerta Covid-19. Osservazioni sull'art. 6, d.l. 28/2020*, in CALZOLAIO E., MECCARELLI M., POLLASTRELLI S. (a cura di), *Il diritto nella pandemia. Temi, problemi, domande*, 2020, pp. 75 e ss.

[76] *"Cross-border data flow in the digital single market: study on data location restrictions"*, *op. cit*. Lo studio, dopo la precisazione che le barriere indirette sono state considerate tali alla luce delle valutazioni fatte da esperti del settore, indica come esempi: l'obbligo di garantire l'accessibilità dei dati a determinate autorità di controllo, l'imposizione di requisiti tecnici generici per i soggetti deputati alla conservazione delle informazioni, l'implementazione di schemi di autorizzazione preventiva per le infrastrutture o i fornitori di servizi e la previsione di restrizioni per le ipotesi di subappalto.

[77] Eloquente l'ipotesi riportata nello studio *ibidem* che, nel tentativo di illustrare la rilevanza che assume la ratio della restrizione nelle operazioni di interpretazione, afferma: "if data should be stored on a server in a specific Member State in order to ensure its accessibility to a national supervisor, then the formal data location requirement can be re-cast into a functional accessibility requirement. However, if the exact same requirement is driven by the

La categoria delle barriere indirette, nonostante i suoi confini piuttosto sfumati, non può essere affatto sottovalutata, dal momento in cui al suo interno si cela la maggioranza degli ostacoli alla libera circolazione dei dati non personali: lo studio citato giunge alla conclusione che, delle quaranta barriere totali rinvenute al termine dell'analisi, trenta rientrano proprio in questa categoria più "sibillina".[78] In realtà, alla luce delle ipotesi analizzate,[79] questo squilibrio non desta troppo stupore: la circostanza che i dati debbano, da un lato, essere obbligatoriamente resi disponibili ai titolari del trattamento o alle autorità di controllo, mentre, dall'altro, non possano essere resi noti a terze parti, unita ai frequenti obblighi di autorizzazione prescritti per poter utilizzare una determinata struttura di archiviazione o un determinato responsabile del trattamento,[80] possono verosimilmente spingere chi accumula queste informazioni a preferire una soluzione domestica – e magari più costosa e meno sicura in termini di conservazione – in luogo di una più funzionale alla propria impresa, ma che potrebbe comportare l'inosservanza dell'ordinamento di riferimento.[81]

Peraltro, la questione degli obblighi di localizzazione permette di individuare una significativa differenza del Regolamento sui dati non personali rispetto al GDPR, consistente nel fatto che gli Stati membri sono i principali destinatari della normativa. Mentre il regolamento riguardante i dati personali concentra la sua attenzione, in primo luogo, sui soggetti che intervengono nella filiera del

need to ensure that data cannot be seized by a third party, then accessibility to a national supervisor is not a sufficient or appropriate translation. Data location as such is not a requirement that can be translated in isolation; the policy objective must be the focus of the translation effort", p. 103.

[78] *Ibid*., p. 6.

[79] *Ibid.*

[80] *Ibid.*

[81] CHANDER A., LÊ U. P., *Data Nationalism*, in *Emory Law Journal*, Vol. 64, Iss. 3, 2015, pp. 677 e ss.

trattamento dei dati – il titolare ed il responsabile del trattamento – stabilendo gli obblighi da rispettare al fine di assicurare una tutela efficiente al *data subject*, il RDNP dedica la sua norma cardine agli Stati membri. D'altronde, non potrebbe essere diversamente giacché, come testimonia la differente base giuridica su cui si fondano, se per il GDPR l'obiettivo (primario) è quello di tutelare un diritto fondamentale dell'individuo, il secondo regolamento si inserisce, invece, in quella serie di strumenti che, incentivando la circolazione, mirano a rafforzare il mercato unico. Ad ulteriore conferma del ruolo di destinatari principali della disciplina ricoperto dai Paesi membri, il testo del Regolamento tiene a precisare che la normativa non è volta né a ridurre le facoltà di scelta delle imprese in relazione alla localizzazione dei dati, le quali rimangono comunque libere di scegliere una soluzione domestica,[82] né l'esternalizzazione dei servizi da parte degli enti pubblici quando sussistono esigenze che li spingono a preferire l'autofornitura.[83]

Come anticipato, la presa di posizione dell'Unione europea nei confronti della *data localization* nell'ambito della circolazione dei dati non personali scaturisce dal preoccupante aumento di misure restrittive verificatosi negli ultimi anni, spesso dettato dalla convinzione che la conservazione e l'analisi dei dati all'interno dei confini nazionali siano sinonimo di sicurezza oppure che facilitino l'accesso e la sorveglianza da parte delle autorità. Senza dimenticare

[82] Regolamento (UE) 2018/1807, cons. n. 4. In particolare: "Il presente regolamento non limita in alcun modo la libertà delle imprese di stipulare contratti che stabiliscano dove devono essere localizzati i dati. Il presente regolamento è inteso unicamente a salvaguardare tale libertà garantendo che il luogo stabilito possa trovarsi ovunque nell'Unione".

[83] Regolamento (UE) 2018/1807, cons. n. 14. In particolare: "Mentre le autorità pubbliche e gli organismi di diritto pubblico sono incoraggiate a considerare i vantaggi economici e di altro tipo dell'esternalizzazione a fornitori esterni di servizi, essi potrebbero avere ragioni legittime per scegliere l'autofornitura di servizi o l'internalizzazione. Di conseguenza, il presente regolamento non obbliga in alcun modo gli Stati membri a subappaltare o esternalizzare la fornitura di servizi che essi intendono fornire direttamente o organizzare con mezzi diversi dagli appalti pubblici".

che alcune limitazioni sono state imposte al preciso scopo di sfavorire i fornitori di servizi stranieri o multinazionali rispetto a quelli nazionali.[84] Stando alle stime prettamente economiche presentate dalla Commissione europea, la drastica diminuzione di queste restrizioni voluta dal nuovo regolamento permetterebbe all'economia dei dati di crescere fino a 739 miliardi di euro entro il 2020.[85] Oltretutto, secondo uno studio dello *European Centre for International Political Economy* (ECIPE), l'effetto sarà più che positivo per il mercato, poiché, beneficiando le industrie di costi minori legati alla maggiore flessibilità nella gestione dei propri dati, il PIL potrebbe crescere di circa 8 miliardi di euro l'anno.[86] Pertanto, la Commissione, al fine di cogliere le opportunità offerte dall'economia dei dati, ha ritenuto necessario garantire il libero flusso delle informazioni stabilendo il medesimo principio di libera circolazione, ma garantendolo tramite due fonti diverse, il GDPR, per il versante dei dati personali e il RDNP, per quello dei dati non personali.[87]

Senonché, volgendo lo sguardo al di là delle valutazioni di carattere prettamente economico sulla cui base, a detta della Commissione europea, è stato giustificato l'intervento teso a

---

[84] *"Cross-border data flow in the digital single market: study on data location restrictions"*, *op. cit.*, p. 17. In particolare: "These barriers can of course take many forms. In some cases, there is a clear and objective compliance requirement behind them, such as a legal obligation to store data locally in order to maintain national control over essential systems and services. In other cases, a barrier can result from business requirements (e.g. customer demand to store data locally), policy preferences (e.g. a desire to keep data within one's own jurisdiction), operational needs (e.g. a requirement to be able to destroy data), or even personal preferences (e.g. favouring local companies) and personal concerns (e.g. concern that foreign entities may seize data stored abroad)".

[85] IDC 2017, *European Data Market Study*, Final Report (SMART 2013/0063).

[86] BAUER M., FERRACANE M. F., LEE-MAKIYAMA H., VAN DER MAREL E., *Unleashing Internal Data Flows in the EU, op. cit*.

[87] Regolamento (UE) 2018/1807, cons. n. 10. In particolare: "Il regolamento (UE) 2016/679 e il presente regolamento forniscono un insieme coerente di norme che disciplinano la libera circolazione di diversi tipi di dati".

contrastare l'aumento delle misure restrittive alla circolazione dei dati, possono scorgersi ulteriori profili che potrebbero aver persuaso le istituzioni dell'Unione ad agire. A tale proposito, una chiave di lettura differente consente di analizzare la questione della *data localization* alla luce del nesso che lega la sovranità digitale alla disponibilità dei dati. Alla dialettica che si instaura fra la circolazione dei dati esternamente e internamente all'Unione fa da sfondo un aspetto che, benché rimasto ancora sottaciuto, ricopre una posizione centrale nel contesto dell'evoluzione del *data law*. Si tratta dei dati a valenza strategica, ossia di quelle informazioni che, in ragione del loro intimo legame con interessi pubblici quali la sicurezza nazionale, lo sviluppo economico e l'ordine sociale, ricoprono una posizione fondamentale per il mantenimento della sovranità statuale e, di conseguenza, spingono gli Stati verso la moltiplicazione dei limiti alla circolazione.[88] Per contro, i benefici di carattere economico enfatizzati dagli organismi europei appaiono spesso come un utile "pretesto" per consentire all'Unione di legiferare in un settore in cui non ha alcuna competenza all'infuori di quella, per l'appunto, economica.

Quanto detto trova conferma in alcune fra le ultime iniziative promosse tanto a livello europeo,[89] quanto a livello nazionale,[90] nella

[88] Come verrà illustrato nel dettaglio nel capitolo finale, la recente proposta di Data Governance Act sembra aver intercettato – benché in maniera ancora acerba – questa tendenza introducendo la categoria dei dati non personali "altamente sensibili" nell'articolo 5 che possono, a titolo esemplificativo riguardare gli obiettivi di politica pubblica dell'Unione europea, la sanità, i trasporti, l'energia, l'ambiente e la finanza.

[89] La proposta congiunta lanciata dai Ministeri dell'economia tedesco e francese di creare una infrastruttura digitale di matrice europea, denominata GAIA-X, rispondente ai valori continentali di sicurezza e tutela dei dati è evidentemente diretta a ridurre la dipendenza nei confronti dei fornitori di servizi non europei e ad incentivare la concorrenza. In tal senso, *GAIA-X: A Pitch Towards Europe. Status Report on User Ecosystems and Requirements*, Federal Ministry for Economic Affairs and Energy (BMWi), 2020.

[90] La predisposizione di una piattaforma unica nazionale per la gestione del sistema di allerta degli utenti della app "Immuni" nell'ambito delle misure di sanità pubblica legate all'emergenza COVID-19 rappresenta una chiara presa di posizione da parte del legislatore

misura in cui hanno come obiettivo la riconquista del terreno perduto dagli ordinamenti giuridici nazionali e sovranazionali in un ambito, quello della gestione dei dati a valenza strategica, in cui la posizione centrale un tempo ricoperta è stata fortemente ridimensionata, oltre che da Stati terzi, anche dall'entrata in campo delle *major* di internet.[91]

L'attrito tra l'anima economica e quella concernente la sovranità è percepibile, in modo particolare, in seno all'articolo 4 del Regolamento (UE) 2018/1807 nella parte in cui prevede come unica eccezione al divieto di imporre obblighi di localizzazione la sicurezza pubblica. Al fine di evitare l'insorgere o il permanere di discipline non fondate su tale base legittima, grava sugli Stati membri il dovere di procedere alla disamina di tutte le norme che impongono un obbligo di localizzazione per poi abrogare quelle non conformi al Regolamento. Tuttavia, nel caso in cui ritengano necessario il mantenimento di alcune misure restrittive, proprio perché fondate su motivi di pubblica sicurezza, devono darne comunicazione alla Commissione europea allegando la relativa giustificazione.[92] Per contro, alla Commissione è riconosciuta la facoltà di presentare osservazioni qualora ritenga opportuno che tali disposizioni debbano essere modificate o addirittura abrogate, in

italiano, il quale ha preferito una soluzione con titolarità pubblica e con infrastrutture localizzate sul territorio nazionale. Per un approfondimento, si rinvia a: COLAPIETRO C., IANNUZZI A., *App di contact tracing e trattamento dei dati con algoritmi: la falsa alternativa tra tutela del diritto alla salute e protezione dei dati personali*, in *Dirittifondamentali.it*, n. 2/2020.

[91] A tal proposito, eloquente è il caso dei Community Mobility Reports messi a disposizione da Google (https://www.google.com/covid19/mobility/) per fornire una panoramica della variazione degli spostamenti della popolazione durante la pandemia causata dalla Covid-19, i quali dimostrano quanto sia pervasiva e vasta la raccolta e l'analisi dei dati realizzata dai servizi OTT.

[92] Regolamento (UE) 2018/1807, art. 4, par. 3 e cons. n. 21. La medesima procedura è prevista al paragrafo 2 nell'eventualità in cui gli Stati intendano introdurre un nuovo obbligo dello stesso tenore.

quanto non confacenti ai principi sanciti dal diritto comunitario [93] o dalla giurisprudenza della Corte di giustizia dell'Unione.[94]

Il considerando n. 19 del RDNP agevola l'interpretazione del significato di sicurezza pubblica. Innanzitutto, il riferimento alla sicurezza sia interna che esterna permette di trattenere tutte le informazioni potenzialmente utili ai fini di prevenzione di attacchi provenienti da Paesi terzi, di fatto legittimando la conservazione di dati relativi a contesti non nazionali o non europei. Appare in tal caso evidente il legame con la speciale disciplina antiterrorismo diffusasi in tutto il continente a seguito degli attacchi terroristici degli anni recenti. Come evidenziato dalla dottrina, il timore di essere vittime di simili aggressioni ha scatenato la proliferazione di normative *ad hoc* che hanno eroso alcuni diritti fondamentali degli individui – soprattutto il diritto alla protezione dei dati personali – in nome della pubblica sicurezza.[95] *A fortiori*, un simile atteggiamento potrebbe contraddistinguere la regolamentazione dei dati non personali: scevro da rischi di lesione diretta ai diritti fondamentali della persona fisica, lo Stato tenterà di trattenere nelle banche dati proprie o, per lo più, dei soggetti sottoposti alla propria giurisdizione quante più informazioni possibili, legittimato dall'interesse alla difesa delle "questioni di incolumità pubblica, in particolare al fine di agevolare le indagini, l'accertamento e il perseguimento di reati".[96]

[93] Regolamento (UE) 2018/1807, art. 4, par. 3 e cons. n. 21.
[94] Per le sentenze della Corte di giustizia dell'Unione europea più rilevanti a tale riguardo, si rinvia alla Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, op. cit.*, p. 13.
[95] RUBECHI M., *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *federalismi.it*, n. 23/2016.
[96] Regolamento (UE) 2018/1807, cons. n. 19. A tale riguardo, il rischio di difformità nelle normative degli Stati membri che potrebbe derivare da questa facoltà di deroga si aggiunge a quello dovuto alla scelta, da parte del legislatore, di ricorrere allo strumento della direttiva per disciplinare il trattamento dei dati personali effettuato da autorità pubbliche in ambito penale. In particolare, ci si riferisce alla Direttiva (UE) 2016/680 relativa alla protezione delle

Nel prosieguo, la normativa sembra ampliare di molto il novero degli interessi legittimanti una deroga. Difatti, nell'esigere una minaccia "reale e sufficientemente grave ad uno degli interessi fondamentali della società", vengono espressamente riportati "il pregiudizio al funzionamento delle istituzioni e dei servizi pubblici essenziali nonché all'incolumità della popolazione, come il rischio di perturbazioni gravi dei rapporti internazionali o della coesistenza pacifica dei popoli, o ancora il pregiudizio agli interessi militari".

In questa definizione a prima vista dettagliata, potrebbero nascondersi non poche insidie interpretative: basti pensare al concetto di servizio pubblico essenziale, il quale, non godendo di una definizione uniforme a livello continentale,[97] rischia di creare una disparità di trattamento tra i diversi Stati membri. Altrettante incertezze accompagnano le nozioni di incolumità pubblica e interessi militari. Se la prima può potenzialmente impedire la circolazione di numerose informazioni relative alla salute dei cittadini – già oggetto di significative barriere indirette secondo lo studio sopra citato –,[98] gli interessi militari, a loro volta, tolgono dalla circolazione, non solo le informazioni *latu sensu* strategiche, ma anche la maggior parte dei dati relativi alla produzione di materiale utilizzato dalle forze armate, detenuti dalle industrie belliche.

---

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 ed alla Direttiva (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 terrorismo e dei reati gravi.

[97] TARANTINO L., *Promozione della concorrenza e disciplina dei servizi pubblici*, 2016, pp. 8-11; DI GIOVANNI A., *I servizi di interesse generale tra poteri di autorganizzazione e concessione di servizi*, in *Nuovi problemi di amministrazione pubblica*, 2018, pp. 1-17.

[98] "*Cross-border data flow in the digital single market: study on data location restrictions*", *op. cit.*

Se questi sono i presupposti, è probabile che gli Stati membri, desiderosi di mantenere le informazioni più delicate nel territorio o nel contesto in cui possono esercitare un potere "diretto", daranno un'interpretazione estensiva al concetto di sicurezza pubblica, al preciso scopo di limitare la fuoriuscita dei dati nella misura più ampia possibile. A tal riguardo, sono condivisibili le perplessità espresse dal Comitato economico e sociale europeo (CESE) con riferimento alla imprecisione con cui viene delineata questa nozione ed alla mancanza di un "riferimento alle controversie o alle modalità per verificare in che modo gli Stati membri rispetteranno i criteri della pubblica sicurezza, né ad eventuali sanzioni nei loro confronti, ove opportuno".[99]

Quanto detto, assume particolare rilevanza a fronte del contesto in cui operano alcune agenzie governative, reso noto a seguito delle rivelazioni riguardanti la vicenda *Datagate*.[100] Questa esperienza ha dimostrato che ad essere interessati al possesso di dati non sono solamente le compagnie private, ma anche le agenzie di *intelligence* che, proprio al fine di garantire la sicurezza pubblica, si sono rese protagoniste di una raccolta massiva di informazioni mai vista nella storia.[101] È bene notare che, nonostante il dibattito manifestatosi in seno all'opinione pubblica a partire dal 2013 si sia concentrato sulla violazione della vita privata degli individui sottoposti a sorveglianza, le stesse osservazioni potrebbero essere svolte, *mutatis mutandis*, in relazione ai dati a carattere non

[99] Parere del Comitato economico e sociale europeo (CESE) sulla "Comunicazione della Commissione al Parlamento europeo e al Consiglio - Linee guida sul regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea" adottato il 25 settembre 2019, pp. 6-7.
[100] NINO M., *Il caso Datagate. I problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy*, in *Diritti umani e diritto internazionale*, vol. 7, 2013, n. 3, pp. 735-737.
[101] FOCARELLI C., *La Privacy. Proteggere i dati personali oggi*, *op. cit.*, pp. 10-16.

personale. Ne è un esempio significativo il comprovato meccanismo in voga fra i funzionari degli organi inquirenti consistente nel chiedere accesso alle informazioni detenute da imprese private nel settore ICT. Richieste che nella maggior parte dei casi non trovano nessuna base giuridica riconosciuta dalla legge e che, solitamente, vengono assecondate per motivi di reverenza o per timore di ripercussioni negative.[102]

In un certo senso, sussiste la possibilità che, grazie allo schermo della sicurezza pubblica, possa venire alla luce anche per i dati non personali una differenziazione già nota per quelli personali. Se il Regolamento generale assicura una disciplina giuridica parzialmente diversa – *rectius*, più stringente – per le cosiddette categorie particolari di dati,[103] è plausibile che in futuro si andrà a delineare una distinzione simile anche per i dati non personali che possiedono un valore strategico. Come si avrà modo di vedere nel corso del capitolo finale, sembra che il legislatore, riprendendo la vecchia nomenclatura,[104] si stia dirigendo verso la creazione di una categoria di dato non personale "sensibile", ossia un dato che per la sua connessione funzionale con l'interesse collettivo della sicurezza pubblica, giustifica un regime giuridico diverso, grazie al quale lo

[102] CATE F. H., KUNER C., MILLARD C., SVANTESSON D. J., *Systematic Government Access to Private-Sector Data Redux*, in *International Data Privacy Law*, vol. 4, 2014. Due eccezioni degne di nota sono quelle di Microsoft ed Apple che si sono opposte alle richieste di accesso da parte delle autorità statunitensi. Al riguardo, si vedano: RUBECHI M., *Sicurezza, tutela dei diritti fondamentali e privacy, op. cit.*, p. 23; OROFINO M., *FBI v. Apple: il caso è (forse) chiuso, ma le questioni di fondo rimangono apertissime*, in *Diritto Pubblico Comparato ed Europeo*, vol. 26, n. 2, 2016, pp. 1-17.

[103] Ci si riferisce all'articolo 9 del Regolamento (UE) 2016/679, rubricato "Trattamento di categorie particolari di dati personali".

[104] Prima dell'abrogazione, la Legge n. 675 del 31 dicembre 1996 relativa alla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, all'articolo 22, riportava la rubrica "Dati sensibili". Anche il Decreto legislativo 30 giugno 2003, n. 196, riportava la medesima dicitura prima della modifica ad opera del decreto legislativo 101 del 2018 relativo alle disposizioni per l'adeguamento della normativa nazionale al Regolamento (UE) 2016/679.

Stato può imporre all'ente che lo conserva, pubblico o privato che sia, un obbligo di localizzazione.[105]

In conclusione, è possibile affermare che la disposizione in parola rappresenta un ulteriore indicatore attestante l'esistenza di una categoria di informazioni di rilievo strategico che, per ora, è sfuggita alla positivizzazione del legislatore europeo, ma che, nella pratica, agita l'intero ordinamento sia a livello sovranazionale che statale. Alla permanente mancanza di riconoscimento di una simile categoria di informazioni che, per la sovranità statale e regionale, sta assumendo un valore essenziale sono riconducibili le problematiche inerenti al trasferimento intra-frontaliero di gruppi di informazioni che, di per sé, stanti il GDPR e il Regolamento 1807 – e salva, chiaramente, l'eccezione prevista dal suo articolo 4 – potrebbero circolare liberamente nell'Unione, ma che, all'opposto, i singoli Stati membri sembrano intenzionati a mantenere all'interno del proprio ambito di controllo, proprio in ragione della loro connessione con la sovranità digitale. In tal senso, le problematiche relative all'insorgenza degli obblighi di *data localization*, insieme alla frammentazione del diritto dei dati che ne è causa, sembrano per lo più ascrivibili alla carenza di un coordinamento unitario a livello europeo nell'ambito della cibersicurezza. La debolezza sistemica che affligge il quadro normativo *in subiecta materia* rappresenta un derivato dell'assetto delle competenze attribuite all'Unione che, forte di una base solida come l'articolo 16 del TFUE, da un lato, e sprovvista di una attribuzione altrettanto valida in materia di

[105] Come verrà illustrato nel prosieguo, un concetto simile è già presente nell'ordinamento giuridico della Repubblica popolare cinese dove vengono in rilievo le nozioni di "*important data*" e la più recente di "*national core data*" le quali, benché possano comprendere sia dati personali che non, approntano una disciplina più rigida proprio in virtù della particolare importanza di queste informazioni rispetto alla sicurezza, all'economia o alla stabilità sociale del Paese. A questo proposito, si veda YUEXIN Z., *Cyber protection of personal information in a multi-layered system*, *op. cit.*, pp. 159-169.

sicurezza digitale, dall'altro, si è trovata costretta a ricorrere all'unico "grimaldello" di competenza a sua disposizione. Difatti, le fonti europee attualmente vigenti in materia di sicurezza nel settore digitale non hanno una base giuridica univoca e spesso sono emanate utilizzando come fondamento disposizioni del TFUE concernenti il mercato interno.[106]

A dispetto di ciò, l'elaborazione di una disciplina organica per un settore eterogeneo come il *data law* non può svilupparsi esclusivamente nella prospettiva del mercato unico, la quale costituisce solamente una delle dimensioni da prendere in considerazione. Se la realizzazione di un'Unione europea tecnologicamente all'avanguardia e capace di competere con Stati Uniti e Cina passa necessariamente per il tramite di una normativa omogenea e armonizzata in materia di dati, appare parimenti vitale che il percorso seguito dalla protezione dei dati personali, culminato con l'introduzione dell'articolo 16 del TFUE e dell'articolo 6 del TUE, venga replicato anche per la sicurezza digitale al fine di colmare una lacuna in tema di competenze unionali che non può che condurre alla parcellizzazione del diritto dei dati e alla contrazione della libera circolazione delle informazioni.

[106] La Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, nota come "Direttiva NIS (Network and Information Security)" e il Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013, noto come "Regolamento sulla cibersicurezza" vantano entrambi l'articolo 114 del TFUE come base giuridica. Le fonti che, invece, hanno carattere principalmente sanzionatorio, come il Regolamento (UE) 2019/796 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri o la Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013 , relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio, sono fondati, rispettivamente, sull'articolo 215 e sull'articolo 83, par. 1 del TFUE.

4.2 Una nuova portabilità autoregolamentata: dalla "*portability*" al "*porting*"

A seguito della risonanza che il diritto alla portabilità dei dati personali ha avuto con l'entrata in vigore del GDPR, anche per il Regolamento sui dati non personali viene sottolineato sin da subito l'impatto positivo che il libero trasferimento delle informazioni da un fornitore di servizi ad un altro, su richiesta dell'utilizzatore e senza costi eccessivi, potrebbe avere nei confronti della concorrenza nel mercato interno.[107] Inoltre, è lo stesso testo della nuova disciplina che effettua una comparazione fra il diritto già vigente nell'Unione – in particolare il GDPR – che garantisce una tutela solida al consumatore desideroso di cambiare il prestatore di servizi, e le lacune che, al contrario, riguardano la situazione in cui versano gli utenti professionali,[108] i quali, sprovvisti di una simile protezione, spesso si trovano intrappolati a causa di pratiche di *vendor lock-in* che comportano oneri di mantenimento più alti e, al contempo, danneggiano la competitività delle imprese.[109]

Sfortunatamente, malgrado le premesse, per il particolare caso dei dati a carattere non personale il legislatore europeo ha deciso di intraprendere una strada diversa rispetto a quanto fatto nel 2016.[110] Se alle persone fisiche è riconosciuto a livello normativo un vero e proprio diritto alla portabilità, gli utenti professionali possono solo fare affidamento sull'elaborazione di codici di condotta frutto di

[107] Regolamento (UE) 2018/1807, cons. n. 29.
[108] L'art. 3, punto 8) del RDNP definisce l'utente professionale come: "una persona fisica o giuridica, compreso un'autorità pubblica e un organismo di diritto pubblico, che utilizza o richiede servizi di trattamento di dati per fini connessi alla sua attività commerciale, industriale, artigianale, professionale o a una sua funzione".
[109] Commissione europea, *Staff Working Document on the free flow of data and emerging issues of the European data economy. Accompanying the document Communication Building a European data economy* (SWD(2017) 2 final), pp. 46-49.
[110] Comunicazione della Commissione, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, op. cit.*, pp. 18-21.

autoregolamentazione la quale, benché supportata e controllata direttamente dalla Commissione, non riuscirà mai a garantire quella certezza del diritto e quella parità di condizioni che dovrebbero essere alla base dell'adozione di questo regolamento.[111] Oltretutto, è difficile comprendere perché ragioni quali la necessità di "mantenere il passo con la potenziale innovazione del mercato e tener conto dell'esperienza e delle competenze dei fornitori di servizi e degli utenti professionali di servizi di trattamento di dati",[112] possano giustificare una regolamentazione tramite codici di condotta in luogo di un vero e proprio diritto che sia in grado di bilanciare lo squilibrio di potere intercorrente tra tali utenti professionali, spesso piccole e medie imprese, e fornitori di servizi *online* che si stanno velocemente trasformando negli attori più potenti del mercato.[113]

La volontà del regolamento di distaccarsi in maniera netta dalla posizione adottata nel GDPR è dimostrata, prima che dalla predisposizione di una tutela giuridica più debole, anche dall'utilizzo di una terminologia differente: se l'individuo può fare affidamento sulla "*portability*" inglese o sulla "*portabilité*" francese, i codici di condotta devono essere orientati alla disciplina, rispettivamente, del "*porting*" o del "*portage*".[114] Questa differenza terminologica deriva, probabilmente, dalla volontà di sottolineare in maniera chiara il tipo di relazione giuridica che viene presa in considerazione nei due testi. Il diritto alla portabilità di cui all'articolo 20 del GDPR fa

[111] Parere del CESE sulla "Comunicazione della Commissione" adottato il 25 settembre 2019, *op. cit.*, pp. 5-9.
[112] Regolamento (UE) 2018/1807, cons. n. 30.
[113] Parere del CESE sulla "Comunicazione della Commissione" adottato il 25 settembre 2019, *op. cit.*, p. 9. Per un'analisi dettagliata del diritto alla portabilità che ne include gli eventuali effetti negativi, anche se con riferimento ai dati personali, si veda: SWIRE P., LAGOS Y., *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, in *Maryland Law Review* 335, 2013, pp. 335-380.
[114] Nelle versioni italiane viene impiegato il medesimo termine, "portabilità", in entrambi i regolamenti.

riferimento ad una situazione giuridica soggettiva in cui i due protagonisti sono, da un lato, l'interessato persona fisica e, dall'altro, colui che tratta le sue informazioni, il quale, di regola, incarna la figura del titolare del trattamento. Dunque, similmente a quanto si è visto nella tradizione statunitense,[115] questo diritto si inserisce in un'ottica di tutela del consumatore nel rapporto con il fornitore del servizio.[116] Per i dati non personali, al contrario, l'articolo 6 circoscrive il suo riferimento non ad un utente generalmente inteso, bensì alla specifica categoria dell'utente professionale, il quale tratta i dati per fini connessi alla sua attività. Di conseguenza, il rapporto intercorrente tra l'utente professionale ed il fornitore di servizi di gestione di dati, più che in una dinamica B2C, può essere ricondotto nell'ambito *business-to-business*,[117] similmente a quanto avviene nel caso di dati personali tra titolare del trattamento e responsabile del trattamento.[118]

Questa soluzione appare, quantomeno, discutibile. La necessità, più volte richiamata, del coinvolgimento delle PMI nel processo di elaborazione di questi codici di condotta non è uno strumento sufficientemente forte da dissuadere i dubbi che pervadono la preferenza per l'autoregolamentazione, soprattutto alla luce dell'attuale momento storico del mercato dei dati in cui poche grandi imprese stanno guadagnando capacità egemoniche. In questo frangente, l'Unione europea ha l'opportunità di distinguersi ancora una volta rispetto ad altre realtà giuridiche tramite una presa di

---

[115] MIGLIETTI L., *Profili storico-comparativi del diritto alla privacy*, *op. cit.*, pp. 8-13.
[116] Comunicazione della Commissione, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, *op. cit.*, pp. 18-21.
[117] *Ibid*.
[118] Il rapporto giuridico sussistente tra utente professionale e fornitore del servizio non sempre può essere declinato all'interno della dinamica titolare-responsabile del trattamento come delineata dal GDPR, poiché l'assunzione di tali ruoli ha luogo solamente se sono coinvolti (anche) dati a carattere personale.

posizione forte verso il riequilibrio di quella parità contrattuale che sembra essersi fortemente indebolita.[119] Proprio da tali esigenze sono di recente nate numerose istanze in ambito accademico volte a sollecitare un dibattito profondo sulla necessità di allargare la normativa a tutela del consumatore al fine di ricomprendere anche le piccole e medie imprese, così da prevenire la formazione di posizioni dominanti che rischiano di alterare la libera concorrenza nel mercato europeo in modo irreversibile.[120] La prevenzione di pratiche simili potrebbe avvenire in maniera più efficace se solo il Regolamento fosse sceso più nel dettaglio, magari fissando a chiare lettere alcune delle norme inderogabili che i codici di condotta dovrebbero necessariamente includere oppure, come ha notato il CESE, definendo gli orientamenti da cui i meccanismi di autoregolamentazione dovrebbero muovere, non limitandosi al semplice richiamo alle migliori pratiche, agli obblighi informativi ed alle tabelle di marcia.[121] Del resto, una maggiore profondità della disciplina emerge ormai nitidamente, specie alla luce dei recenti interventi promossi dalle istituzioni dell'Unione, i quali, come verrà illustrato nel capitolo quarto, riportano l'impatto esiguo che i codici

[119] Parere del CESE sulla "Comunicazione della Commissione" adottato il 25 settembre 2019, *op. cit.*, p. 4.
[120] DREXL J., *Designing Competitive Markets for Industrial Data – Between Propertisation and Access*, Max Planck Institute for Innovation & Competition Research Paper No. 16-13, 2016, pp. 55-66; FIA T., *La tutela dei dati non personali: accesso, proprietà e regolamentazione*, in *Nuovo Notiziario Giuridico*, 2019, pp.125-126; Parere del CESE sulla "Comunicazione della Commissione" adottato il 25 settembre 2019, *op. cit.*, p. 9.
[121] MONTAGNANI M. L., *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, *op. cit.*, pp. 304-310; Parere del CESE sulla «Proposta di regolamento», *op. cit.*, pp. 5-6. In particolare: "In questo senso, il CESE ritiene che il regolamento all'esame dovrebbe almeno fornire un insieme di norme di base relative ai rapporti contrattuali tra i fornitori di servizi e gli utenti e prevedere una lista nera di clausole vietate a causa della limitazione del diritto di portabilità, secondo i parametri indicati in particolare nel suo parere sull'autoregolamentazione e sulla co-regolamentazione. Tuttavia, è inconcepibile che la Commissione non abbia neppure proposto di definire «orientamenti» per l'elaborazione dei codici di condotta precedentemente citati, come ha già fatto in altri settori, sostenuta in questo approccio dal CESE".

di condotta finora approvati, segnatamente quelli concernenti i servizi *cloud*,[122] sono riusciti a produrre sulle dinamiche di mercato, fra i motivi a sostegno di un nuovo provvedimento in materia di dati.[123]

5. Tessere mancanti nel mosaico regolamentare europeo?

Le iniziative intraprese dall'Unione europea nel corso dell'ultimo decennio hanno gradualmente completato il variegato mosaico del mercato europeo digitale. Invero, le soluzioni di compromesso e le ampie lacune emerse al termine dell'*iter* legislativo che ha portato alla approvazione della disciplina del flusso dei dati non personali mostrano l'incompletezza di questo grande disegno.[124]

In particolare, alcuni dei punti deboli della normativa in esame derivano da un contrasto che, benché preso in considerazione dal legislatore, non sembra essere stato risolto con una scelta adatta alle problematiche che titolari, responsabili del trattamento e gestori dei dati in genere si trovano ad affrontare quotidianamente. I regolamenti, le direttive e tutte le altre fonti, anche di *soft law*, adottate al fine di rendere l'economia dei dati alla portata di tutti

[122] Ci si riferisce ai codici di condotta per facilitare il passaggio dei dati tra servizi *cloud* SWIPO (Switching Cloud Providers and Porting Data) i quali vengono definiti nella relativa pagina web (https://swipo.eu/) come: "a multi-stakeholder group facilitated by the European Commission, in order to develop voluntary Codes of Conduct for the proper application of the EU Free Flow of Non-Personal Data Regulation / Article 6 "Porting of Data".

[123] La Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati), 23 febbraio 2022 (Com(2022)68 final), recita a p. 4: "Rispetto ai servizi cloud, poiché l'approccio di autoregolamentazione non sembra aver inciso in modo significativo sulle dinamiche del mercato, la presente proposta prevede un approccio normativo al problema evidenziato nel regolamento sulla libera circolazione dei dati non personali".

[124] È condivisibile a tale proposito l'osservazione secondo la quale è "anche dall'efficacia del Regolamento [sulla libera circolazione dei dati non personali] che si misura quella dell'intero quadro regolatorio sulla libera circolazione dei dati", in MONTAGNANI M. L., *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, *op. cit.*, p. 304.

sembrano essere lontane da una realtà dei fatti poliedrica ed interconnessa come quella odierna, con la conseguenza che quando differenti mondi entrano in contatto l'uno con l'altro tutto l'impianto normativo viene messo a dura prova. In tal senso, il pomo della discordia da cui promanano le falle del sistema sembra risiedere nel differente peso attribuito al concetto di rischio nei due regolamenti, il quale, creando un dislivello alla base della normativa europea in materia di dati, contribuisce a rendere fragile l'intera struttura. Se il *risk-based approach* costituisce uno degli elementi qualificanti il Regolamento generale sui dati personali,[125] la stessa cosa non può dirsi con riferimento alla disciplina dei dati non personali, dove la valutazione del rischio, che si rivelerebbe uno strumento assai utile per comprendere la natura del dato e per individuare le implicazioni che i dati non personali possono avere sulla generalità dei trattamenti realizzati dal medesimo soggetto, non viene presa in dovuta considerazione.[126] Difatti, come si tenterà di illustrare nella parte relativa alla questione definitoria, la decisa accelerazione della digitalizzazione della società moderna ha messo in crisi la definizione stessa di dato personale, portando con sé innumerevoli difficoltà nell'individuazione della linea di confine tra carattere personale e non personale e causando non pochi disagi tanto ai titolari del trattamento quanto alle autorità di controllo che devono monitorarli.[127] Pertanto, in un mondo come quello dei dati, dove la

[125] GIANNONE CODIGLIONE G., *Risk-based approach e trattamento dei dati personali*, in SICA S., D'ANTONIO V., RICCIO G. M., *La nuova disciplina europea sulla privacy*, 2016, pp. 55-78; MANTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le Nuove Leggi Civili Commentate*, 1/2017, pp. 144-164.
[126] FINCK M., PALLAS F., *They who must not be identified – distinguishing personal from non-personal data under the GDPR*, in *International Data Privacy Law*, 2020, Vol. 10, No. 1, pp. 11-36.
[127] DUCATO R., *La crisi della definizione di dato personale nell'era del web 3.0. Una lettura civilistica in chiave comparata*, in CORTESE F., TOMASI M. (a cura di), *Le definizioni nel diritto. Atti delle giornate di studio 30-31 ottobre 2015*, 2016, pp. 160-164.

natura delle informazioni cambia frequentemente, non è più possibile limitare la valutazione del rischio – generalmente inteso e non limitato esclusivamente alla c.d. "valutazione d'impatto sulla protezione dei dati" prevista dall'art. 35 del GDPR – alle sole ipotesi di dati personali, ma appare opportuno, se non necessario, estenderla a tutti i dati che il medesimo soggetto ha a disposizione, includendo anche quelli non personali. Purtroppo, è proprio l'assenza di una visione onnicomprensiva, capace di tenere conto della mutevolezza della realtà digitale a minare l'efficacia delle disposizioni del RDNP.

In sintesi, l'economia globale ed interconnessa che caratterizza la nostra epoca si basa su un incessante scambio di informazioni che partono ed arrivano in tutte le parti del mondo in tempi praticamente nulli. In risposta al rapido aumento del valore economico e dell'importanza strategica dei dati, sia personali che non, gli Stati hanno dimostrato un atteggiamento di chiusura, sfociato poi nell'adozione di normative aventi ad oggetto obblighi di localizzazione. Di fronte ad un cambiamento di simile portata, l'ordinamento giuridico europeo ha deciso fronteggiare la sfida posta dal fenomeno della *data localization* non attraverso un'iniziativa singolare ed unica, ma seguendo un percorso a tappe, in linea con la gerarchia di valori della tradizione giuridica continentale. In prima battuta, il legislatore ha deciso di predisporre una tutela elevata all'interno dell'Unione europea per quanto riguarda il trattamento dei dati personali. Partendo da tale presupposto, ha poi elaborato un insieme di regole che, per un verso, incentivasse la circolazione di tali dati sul suolo continentale e, per l'altro, permettesse alla tutela di viaggiare con il dato personale anche quando questo viene trasferito verso Paesi terzi.

La disciplina riguardante l'altro versante del *data law*, quello del dato non personale, ha visto la luce in un secondo momento,

quando il peso della mancanza di una normativa completa a sostegno dell'economia europea dei dati non era di fatto più sostenibile. Sfortunatamente, il Regolamento sulla libera circolazione dei dati non personali non sembra avere soddisfatto le aspettative, in quanto non riesce a fornire un quadro disciplinare sufficientemente aderente alle dinamiche della realtà digitale.

Allargando lo sguardo alla normativa generale, si può osservare una carenza di una risistemazione in chiave organica di tutta la disciplina dei dati. Attualmente, l'ordinamento continentale consta di una vasta gamma di normative settoriali e, in alcuni casi, non coordinate, la cui stratificazione nel corso dell'ultimo decennio rischia di confondere l'interprete e di tradursi in uno strumento non adatto a servire lo sviluppo della società digitale.[128] Le lacune patite dal Regolamento sui dati non personali non rappresentano altro che il precipitato ultimo di questa disordinata ipertrofia normativa: nonostante l'apparente complementarietà, le sue disposizioni sono state concepite come facenti parte di un *corpus* separato rispetto al Regolamento generale sulla protezione dei dati personali, in evidente contrasto con quella visione di insieme che è ormai imprescindibile se si vuole regolamentare il mondo virtuale con la speranza di ottenere risultati concreti. Viceversa, il RDNP rischia di diventare un regolamento "senza oggetto" in quanto l'assenza di una impostazione sistemica non permette di inquadrare il problema nella prospettiva idonea ad attribuire ai dati non personali e alla relativa disciplina l'importanza che meritano. In aggiunta, oltre alla preponderanza schiacciante del GDPR subita dal Regolamento sui dati non personali, non sono da sottovalutare le ulteriori problematiche concernenti il rapporto fra queste due fonti e le altre discipline

[128] MONTAGNANI M. L., *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, *op. cit.*, pp. 311-313.

settoriali che, spesso, prescindono dalla distinzione personale-non personale.[129]

La risoluzione degli interrogativi che inevitabilmente emergono da questo scarso coordinamento normativo è posta totalmente a carico del soggetto che gestisce i dati, il quale, disorientato in un labirinto di regole, si rifugerà nei lidi più sicuri, ma anche più costosi e rischiosi, dell'internalizzazione del trattamento dei dati. Tuttavia, è bene ricordare, simili pratiche non sono sostenibili da parte delle piccole e medie imprese che, ancora una volta, saranno costrette a pagare le conseguenze di disposizioni normative poco chiare.

[129] Parere del CESE sulla "Comunicazione della Commissione" adottato il 25 settembre 2019, *op. cit.*, p. 8.

CAPITOLO III

LA QUALIFICAZIONE DEL "DATO" SECONDO I CRITERI DELL'ORDINAMENTO EUROPEO

Sommario: 1. Introduzione. 2. La definizione ampia di dato personale. 2.1. Le articolazioni del dato personale. 2.2. Gli elementi costitutivi del dato personale. 3. Il dato non personale. 3.1. Il dato anonimizzato. 3.1.1. Anonimizzazione e rischio di re-identificazione. 3.1.2. Il design del trattamento residuo in chiave contestuale. 3.2. Il dato industriale e la questione della proprietà. 3.2.1. Le soluzioni *de iure condito*: le normative vigenti. 3.2.2 La regolazione della *data economy* tra proprietà ed accesso. 4. Dagli insiemi di dati misti al "Data by Design". 5. Verso la regolamentazione di un sistema integrato di gestione dei dati.

1. Introduzione

La *summa divisio* che segna il panorama legislativo europeo richiede al giurista una fine capacità di riconoscimento delle due macrocategorie che compongono il mondo dei dati. Una distinzione giuridicamente qualificata tra dato personale e dato non personale si rivela fondamentale al fine di conciliare due valori apparentemente antitetici quali la tutela dei diritti fondamentali dell'individuo e la libera circolazione delle informazioni all'interno del territorio europeo. Un erroneo inquadramento del concetto di dato personale potrebbe produrre indebite ripercussioni tanto su diritti individuali costituzionalmente garantiti, i quali verrebbero menomati da una interpretazione troppo restrittiva, quanto sulla oramai

imprescindibile dimensione dello scambio di dati, che risulterebbe afflitta da una lettura indebitamente estensiva della fattispecie.

Il quadro vigente fonda l'applicabilità delle rispettive discipline sulla preventiva verifica della natura del dato trattato. Conseguentemente, il requisito preliminare che si pone all'attenzione dei titolari del trattamento, ai fini dell'individuazione della cornice normativa di riferimento, concerne la corretta qualificazione dei dati a loro disposizione.[1]

L'approfondimento dei profili definitori della materia, oggetto del presente capitolo, svelerà una realtà ben più complessa e poliedrica di quanto il legislatore lasci intendere.[2] L'impostazione statica che spesso traspare dall'azione delle istituzioni continentali si scontra con l'inarrestabile avanzamento della tecnologia. In tal senso, l'apporto del giurista risulta essere imprescindibile in un momento storico in cui la caratterizzazione del dato viene costantemente messa in discussione da strumenti di analisi progettati per individuare collegamenti invisibili fra dati, con l'obiettivo di estrarre informazioni nuove e di maggior valore. In virtù di ciò, si corre il rischio concreto che la definizione, o persino la concezione generale, dei dati personali e non personali proposta dalla normativa europea necessiti di alcune rivisitazioni in risposta alle problematiche derivanti dall'avvento della digitalizzazione e dell'intelligenza artificiale.

Il presente capitolo si aprirà con l'analisi della nozione di dato personale, andando ad approfondire sia i suoi elementi costitutivi, che le diverse sottoclassi che si evincono dalla disciplina vigente. In

[1] AGCM, AGCOM, Garante per la protezione dei dati personali, *Indagine conoscitiva sui big data*, 2018, pp. 8-10.
[2] FINCK M., PALLAS F., *They who must not be identified – distinguishing personal from non-personal data under the GDPR*, in *International Data Privacy Law*, 2020, Vol. 10, No. 1, p. 12.

un secondo momento, il nesso inscindibile che il legislatore ha voluto imprimere tra tale prima categoria di dati e quella dei dati non personali, i quali, per l'appunto, sono definiti in negativo, impone di procedere con l'esame del secondo gruppo di informazioni, nel tentativo di individuare le gradazioni e le peculiarità che lo contraddistinguono. Il parallelo è stato sviluppato con l'obiettivo di fare luce sull'effetto a cascata che la "trasformazione" del dato personale, causata dallo sviluppo di nuove metodologie di raccolta e analisi delle informazioni, genera nei confronti della connessa categoria del dato non personale. Le problematiche evidenziate nel contesto della presente disamina sembrano indicare che per stare al passo con lo sviluppo tecnico potrebbe essere necessario riconsiderare la concezione europea di dato personale e di dato non personale.

2. La definizione ampia di dato personale

Il nucleo della definizione di dato personale rimane costante in tutti i testi normativi vigenti in Europa. Con riguardo alla disciplina attualmente vigente, tanto il GDPR quanto la Convenzione n. 108 del 1981 si riferiscono al dato a carattere personale come "qualsiasi informazione riguardante una persona fisica identificata o identificabile". [3] Se si eccettua una trascurabile variazione terminologica presente nella versione italiana della normativa, [4] il nocciolo della definizione è rimasto invariato rispetto a quanto previsto dalla abrogata Direttiva 95/46/CE.

[3] L'inciso riportato fa riferimento all'art. 4, punto 1) del GDPR. L'art. 2, lett. a) della Convenzione 108 definisce il dato personale come "ogni informazione concernente una persona fisica identificata o identificabile («persona interessata»)".
[4] Il sintagma inglese "relating to" è stato tradotto con il termine "concernente" nella Direttiva 95/46/CE e come "riguardante" nel Regolamento 2016/679.

Tuttavia, proseguendo nella lettura del primo punto dell'articolo 4 del regolamento è percepibile una forte aspirazione all'aggiornamento della nuova disciplina. [5] Nel tentativo di specificare il concetto di "identificabilità", il legislatore del 2016 aggiunge tre riferimenti ulteriori rispetto a quelli inseriti undici anni prima. Si tratta dei dati relativi all'ubicazione, degli identificativi online e dell'identità genetica. [6] Dunque, già attraverso queste modeste modifiche il regolamento offre una prima importante chiave interpretativa: il progresso tecnologico impone una lettura moderna della categoria del dato personale che deve ricomprendere tutte quelle informazioni che oggi, a differenza di quanto accadeva in passato, hanno assunto un rilievo quantitativo e qualitativo smisurato. Di conseguenza, l'articolato proposto dal legislatore si presta intenzionalmente ad interpretazioni estremamente espansive, arrivando ad includere qualsiasi informazione che consente di individuare una specifica persona fisica, distinguendola dagli altri appartenenti ad una determinata collettività.[7]

Già nella vigenza della normativa anteriore, la giurisprudenza aveva sfruttato il margine ermeneutico garantito dalla disciplina muovendosi sempre verso l'orizzonte dell'allargamento del novero delle informazioni qualificabili come personali. In prima battuta, la Corte di giustizia ha escluso, ai fini dell'applicazione delle regole poste a tutela delle informazioni concernenti un individuo, la necessità della sussistenza di un nesso diretto con l'esercizio delle

[5] COLAPIETRO C., *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *federalismi.it*, n. 2/2018, pp. 13-19.
[6] Gli identificativi online ed i dati genetici vengono definiti con maggiore dettaglio, rispettivamente, nei conss. n. 30 e n. 34 del GDPR.
[7] DUCATO R., *La crisi della definizione di dato personale nell'era del web 3.0. Una lettura civilistica in chiave comparata*, in CORTESE F., TOMASI M. (a cura di), *Le definizioni nel diritto. Atti delle giornate di studio 30-31 ottobre 2015*, 2016, pp. 150-154.

libertà fondamentali garantite dai Trattati.[8] Successivamente, la medesima Corte, sulla scorta di quanto fatto in precedenza dalla Corte di Strasburgo,[9] si è prodigata al fine di non circoscrivere l'area di applicabilità della Direttiva Madre ai dati legati alla vita privata dell'interessato, ma, al contrario, ha qualificato come parimenti rilevanti informazioni attinenti alle altre dimensioni della vita dell'individuo, fra cui la vita professionale, sulla scorta delle possibilità di identificazione univoca che esse offrono.[10] D'altro canto, un parziale arresto della costante crescita della nozione di dato personale sembra verificarsi nella causa *YS*, nel contesto della quale i giudici europei hanno escluso che l'analisi giuridica inclusa in una bozza di decisione redatta dal funzionario del servizio dell'immigrazione olandese relativa alle domande di permesso di soggiorno costituisse, di per sé, un'informazione di carattere personale. La Corte afferma che, a differenza dei dati personali presenti nella valutazione del funzionario e sui quali la stessa si fonda, l'analisi giuridica può solamente assurgere ad informazione riguardante l'applicazione della norma astratta al fatto concreto da parte dell'autorità competente, ma non a dato personale in relazione al quale è possibile esercitare il diritto di accesso previsto dalla direttiva.[11] Malgrado tale trascurabile interruzione, l'opera di ampliamento per via esegetica riprende poco dopo, in risposta ad una questione pregiudiziale riguardante l'esatta qualificazione delle risposte scritte fornite da un candidato durante lo svolgimento di un

[8] Corte di Giustizia, 20-5-2003, cause riunite C-465/00, C-138/01 e C-139/01, Rechnungshof *c*. Österreichischer Rundfunk e altri e Christa Neukomm e Joseph Lauermann *c*. Österreichischer Rundfunk, par. 43.
[9] Corte europea dei diritti umani, sentenza Amann c. Svizzera (GC), n. 27798/95, 2000 – II.
[10] Corte di Giustizia, 9-11-2010, cause riunite C-92/09 e C-93/09, Volker und Markus Schecke GbR.
[11] Corte di Giustizia, 17-7-2014, cause riunite C-141/12 e C-372/12, YS *c*. Minister voor Immigratie, Integratie en Asiel, e Minister voor Immigratie, Integratie en Asiel *c*. M, S, parr. 37-48.

esame professionale e delle relative annotazioni dell'esaminatore.[12] I giudici concludono per l'attribuzione dello *status* di dato personale tanto per le risposte del candidato quanto per le annotazioni dell'esaminatore sulla base della accezione estesa che il legislatore ha voluto conferire per mezzo della formulazione dell'articolo 2, lett. a) della Direttiva Madre.[13]

La medesima direttrice di allargamento dell'ambito operativo della normativa è stata seguita anche a livello nazionale. La Corte di Cassazione italiana è spesso intervenuta con l'intento di estendere l'applicazione del d.lgs. 196 del 2003 (meglio noto come Codice Privacy),[14] nel corso di vicende in cui i giudici di prime cure o i ricorrenti avanzavano teorie a sostegno di un orientamento più restrittivo.[15]

A ben vedere, l'interpretazione in senso ampio della categoria del dato personale trova ispirazione non solo nell'articolo 4, ma anche nel considerando n. 26 del GDPR.[16] Tale inciso, malgrado la sua collocazione nel preambolo, ha assunto carattere dirimente in merito alla corretta individuazione della natura dei dati. Esso traccia la dicotomia tra dati a carattere personale e informazioni anonime nel momento in cui mira a definire in concreto il concetto di

[12] Corte di Giustizia, 20-12-2017, causa C-434/16, Peter Nowak *c*. Data Protection Commissioner.
[13] *Ibid*., par. 34.
[14] Decreto legislativo 30 giugno 2003, n. 196 recante il "Codice in materia di protezione dei dati personali" (G.U. 29 luglio 2003, n. 174).
[15] Cass. civ., sez. II, 02/09/2015, sent. n. 17440. In tale caso, la corte ha ritenuto, contrariamente a quanto fatto dal tribunale di primo grado, che la ripresa delle immagini degli avventori di un locale commerciale costituisse dato personale, indipendentemente dal fatto che la videosorveglianza fosse accompagnata da concomitante registrazione. Inoltre, si veda Cass. civ., sez. II, 05/07/2018, sent. n. 17665, dove la corte respinge la tesi di parte ricorrente che proponeva una divisione giuridica tra dati personali e dati meramente identificativi, secondo una motivazione che qualificava i secondi semplicemente come *species* del *genus* rappresentato dalla ampia categoria di dati.
[16] La parte del considerando n. 26 relativa alla ragionevolezza dei mezzi utilizzati per procedere all'identificazione costituisce lo sviluppo di quel principio già presente, *in nuce*, nel considerando n. 26 della Direttiva 95/46/CE.

"identificabilità", ossia il fattore che rende un dato personale in tutte le ipotesi in cui sono presenti mezzi di cui il titolare del trattamento o un terzo possono ragionevolmente avvalersi al fine di portare a termine l'identificazione di una persona fisica. Come si vedrà in maniera più approfondita nel prosieguo, la vocazione altrettanto estensiva desumibile dal considerando n. 26 non può che spingere il giurista ad assecondare una volontà legislativa che si dimostra più che chiara.[17]

Anche in questo caso, la Corte di giustizia conferma di non essere contraria ad una interpretazione in linea con la *ratio* di ampliamento della legge. La vicenda da cui scaturisce il caso *Breyer* concerne la qualificazione della natura degli indirizzi IP dinamici generati in occasione della consultazione dei siti internet dei servizi federali tedeschi e conservati per finalità di contrasto della pirateria informatica.[18] Le circostanze sono propizie per dare contenuto alla formula "l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona",[19] in quanto sono coinvolti, oltre al *data subject*, altri

[17] Oltre che dalla lettera della legge, la volontà del legislatore risultava evidente già dai documenti prodromici all'approvazione della Direttiva Madre. Ad esempio, la proposta modificata della Commissione europea recita: "The amended proposal meets Parliament's wish that the definition of "personal data" should be as general as possible, so as to include all information concerning an identifiable individual" (cfr. Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(92) 422 final), 15-10-1992, p. 9).

[18] Corte di Giustizia, 19-10-2016, causa C-582/14, Patrick Breyer *c*. Bundesrepublik Deutschland. Come illustrato dalla sentenza in parola, gli indirizzi IP dinamici sono sequenze numeriche assegnate ad un computer per mezzo delle quali è consentita la comunicazione fra differenti terminali collegati alla rete. Essi si distinguono dagli indirizzi IP "statici", permanentemente associati ad un dispositivo, per via della loro provvisorietà, la quale, comportando un cambiamento di indirizzo ad ogni connessione, non permette di associare, in via diretta, un determinato computer al collegamento fisico alla rete. A tale proposito, si vedano i parr. 15 e 16.

[19] L'inciso coincide con quello del considerando n. 26 della Direttiva 95/46/CE sul quale si è pronunciata la Corte. Tuttavia, al fine di evitare equivoci, è bene precisare che con la nozione "responsabile del trattamento" si intende il moderno "titolare del trattamento"; terminologia che in Italia è stata introdotta con il Regolamento (UE) 2016/679.

due soggetti che trattano i dati. Da una parte, si trova il fornitore di servizi di media online, nel caso di specie coincidente con la Repubblica federale di Germania, che, oltre all'indirizzo IP, registra dati quali nome del sito consultato, parole inserite nei campi di ricerca, data e ora della consultazione, volume dei dati trasferiti e messaggio relativo all'esito della consultazione. L'insieme di tali informazioni non permette però al fornitore di servizi di risalire in via autonoma, ossia senza l'ausilio di dati aggiuntivi detenuti da altri, all'identità dell'utente, salvo che non sia quest'ultimo ad inserire volontariamente i dati relativi alla propria identità. Dall'altra parte, invece, opera il fornitore di accesso ad internet che assegna l'indirizzo IP all'utente abbonato e che, pertanto, può giungere all'identificazione in maniera piuttosto agevole.[20] La pronuncia emanata dalla corte nazionale tedesca, che rigettava la domanda dell'appellante concernente l'inibizione della conservazione dell'indirizzo IP al fornitore del servizio di media, si fondava su una lettura restrittiva dell'insieme dei mezzi di cui il titolare si sarebbe potuto servire. La necessità di fare ricorso ad un altro soggetto al fine di ricostruire l'identità dell'interessato escludeva la qualifica di dato personale dell'indirizzo IP dinamico per difetto del requisito di identificabilità.[21]

L'esegesi proposta dalla corte nazionale viene confutata dalla differente prospettiva, incentrata sul contesto interconnesso in cui operano i titolari del trattamento moderni, adottata dalla Corte di giustizia per valutare la nozione di "mezzi utilizzabili". Secondo la

[20] Con specifico riferimento ai fornitori di accesso ad internet, la qualifica di dato personale per gli indirizzi IP era già stata stabilita dalla Corte in Corte di Giustizia, 24-11-2011, causa C-70/10, Scarlet Extended SA *c*. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). Per un approfondimento, si veda: CALZOLAIO S., *Gli ISP si salvano nel P2P. Ma reggeranno allo streaming?*, in *Forum di Quaderni costituzionali*, 2012, pp. 1-8.
[21] Corte di Giustizia, causa C-582/14, Breyer, *cit.* par. 21.

logica seguita dai giudici europei, il riferimento, oltre che al titolare del trattamento, agli "altri" soggetti cui è possibile fare affidamento ai fini dell'identificazione impone di prendere in considerazione non solo l'ambito di operatività del titolare, ma anche tutti i canali che questo può, ragionevolmente, aprire verso soggetti terzi allo scopo di portare a termine tale identificazione. Non assume rilievo *ex se* escludente della natura di dato a carattere personale la mera circostanza che le informazioni necessarie ad individuare il *data subject* si trovino nella disponibilità di più titolari del trattamento.[22] Nel caso di specie, la Corte conclude per la personalità dell'indirizzo IP dinamico proprio perché ravvisa nella astratta possibilità riconosciuta al fornitore di servizi di media di "rivolgersi, in particolare in caso di attacchi cibernetici, all'autorità competente affinché quest'ultima assuma le iniziative necessarie per ottenere tali informazioni dal fornitore di accesso a Internet e per avviare procedimenti penali" uno dei mezzi ragionevoli cui può fare ricorso.[23]

In conclusione, il carattere egemonico che contraddistingue la categoria del dato personale rispetto a tutte le altre informazioni deriva tanto da una nozione concepita, già in principio da parte del legislatore, in maniera decisamente ampia e da un fattivo lavoro di una giurisprudenza che, da un lato, si è dimostrata molto più attenta alle esigenze di tutela del diritto fondamentale alla protezione dei dati relativi alle persone fisiche piuttosto che alla libera circolazione, mentre dall'altro, ha dovuto necessariamente tenere conto dell'evoluzione del contesto tecnologico.

[22] *Ibid*. parr. da 42 a 44.
[23] *Ibid*. par. 47.

2.1 Le articolazioni del dato personale

Una norma definitoria di così ampio respiro non implica necessariamente una regolazione equivalente per tutte le informazioni da essa contemplate. Lo stesso Regolamento generale propone una distinzione normativamente qualificata all'interno della categoria dei dati personali nel momento in cui predispone una disciplina più onerosa per le cosiddette "categorie particolari di dati" e per i dati "relativi a condanne penali e reati". Il divieto generale di trattamento di informazioni particolari posto dal primo comma dell'articolo 9 del GDPR, da un lato,[24] e il controllo dell'autorità pubblica e le ulteriori garanzie prescritte per i dati relativi alle condanne penali, ai reati o a misure di sicurezza, prescritti dall'articolo 10, dall'altro, riflettono la particolare premura che viene richiesta per il trattamento di tali sottoinsiemi di informazioni personali. In ragione della loro sensibilità e dei maggiori rischi di lesione per i diritti e le libertà fondamentali degli individui derivanti dalla loro elaborazione,[25] il regolamento inasprisce le condizioni che ne legittimano il trattamento, aprendo di fatto le porte ad una divisione fra dati comuni e dati particolari sottoposti ad un regime parzialmente più restrittivo.[26] Tale peculiarità sembra in un certo

[24] I dati che rientrano nelle "categorie particolari" sono quelli che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
[25] Regolamento (UE) 2016/679, cons. n. 51.
[26] Le particolari regole che disciplinano il trattamento delle categorie particolari di dati concernono, innanzitutto, le deroghe al divieto generale di trattamento previste all'art. 9, par. 2 del GDPR, il quale, in sostanza, prescrive delle basi giuridiche alternative rispetto a quelle sancite dall'art. 6 per i dati comuni. Ulteriori limiti sono introdotti per l'adozione di una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione (art. 22, par. 4). Per i dati personali relativi a condanne penali e reati di cui all'art. 10, il trattamento è ammesso solamente sotto il controllo dell'autorità pubblica o se autorizzato da norma di legge che preveda garanzie appropriate per i diritti e le libertà degli interessati. Inoltre, entrambe le categorie di dati in parola sono accomunate dalla prescrizione di obblighi aggiuntivi per i titolari ed i responsabili nelle ipotesi in cui il loro trattamento avvenga su

senso proporre una rivisitazione di quella "teoria delle sfere" messa da parte dal Tribunale costituzionale tedesco nel 1983, sulla base di una lettura orientata ad un giudizio di pericolosità. Il legislatore introduce una tutela multilivello che dipende dalla sfera del rischio sottesa al trattamento di una determinata tipologia di informazioni. Sulla scorta di una presunzione (quasi assoluta) di lesività per i diritti individuali, la valutazione generale del rischio che il legislatore svolge a monte palesa un collegamento tra gli ambiti di interesse cui sono riconducibili i dati dell'articolo 9 e dell'articolo 10 e quella dimensione intima della vita dell'individuo che la teoria delle sfere mirava a proteggere più intensamente. Dunque, la catalogazione offerta dal GDPR attesta il mancato raggiungimento di una vera equiparazione nella qualificazione dei dati personali come prospettata dalla Consulta tedesca nella sentenza sul censimento.[27]

D'altronde, sembra estremamente arduo giungere ad un approdo simile in ragione della genesi del diritto alla protezione dei dati personali, caratterizzata da una costante contaminazione da parte del limitrofo diritto alla vita privata: sebbene il trattamento di tutti i dati a carattere personale sia protetto dallo scudo dell'articolo 8 della Carta dei diritti fondamentali, quei dati dalla cui analisi può conseguire anche una lesione del rispetto alla vita privata sancito all'articolo 7, vengono percepiti in maniera differente. Eloquenti in tal senso furono le conclusioni dell'Avvocato generale Cruz Villalón esposte in occasione del caso *Digital Rights Ireland*, incentrate sul tentativo di avanzare una distinzione tra "dati personali in quanto

larga scala. Fra questi, si segnalano gli obblighi di designazione di un rappresentante nell'Unione (art. 27, par. 2, *lett*. a)), di tenuta del registro delle attività di trattamento anche quando l'impresa o l'organizzazione abbia meno di 250 dipendenti (art. 30, par. 5), di svolgimento della valutazione di impatto sulla protezione dei dati (art. 35, par. 3, *lett*. b)), di nomina di un responsabile per la protezione dei dati (art. 37, par. 1, *lett*. c)).

[27] *Supra* cap. I, par. 2.

tali", per i quali sono sufficienti le garanzie prestate dall'articolo 8, e "dati più che personali" che si caratterizzano per il loro legame con gli aspetti afferenti alla vita privata della persona.[28] Il ragionamento dell'Avvocato generale, che richiama espressamente concetti quali "sfera intima", "sfera privata" e "sfera personale", mira a sostenere la necessità di differenziazione nel trattamento e nella disciplina dei "dati più che personali", atteso che la cristallizzazione della vita privata degli individui in forma di dati analizzabili con mezzi informatici pone un problema "a monte", ossia preliminare rispetto a quello del trattamento e delle garanzie stabilite dall'articolo 8 della Carta. Esistono dati, insomma, la cui elaborazione risulta di per sé pericolosa.[29]

Il GDPR sembra fare propria la medesima logica per mezzo dei citati articoli 9 e 10 e crea una spaccatura in seno alla categoria dei dati personali.[30] Tuttavia, come per ogni divisione introdotta nel complesso mondo delle informazioni, anche questa scelta legislativa rischia di aggiungere un ulteriore grado di complessità nelle operazioni di qualificazione delle informazioni a cui il titolare del trattamento dovrà porre particolare attenzione.

Per converso, è possibile individuare un'ulteriore classe di dati che si caratterizza per il regime di maggiore favore cui, potenzialmente, è possibile accedere. I dati sottoposti ad un processo di pseudonimizzazione non sono espressamente definiti nel

[28] Conclusioni dell'Avvocato generale Cruz Villalón del 12 dicembre 2013, Digital Rights Ireland Ltd (C-293/12) *c*. Minister for Communications, Marine and Natural Resources e altri e Kärntner Landesregierung (C-594/12) e altri, parr. 59-67.
[29] *Ibid.*
[30] È opportuno segnalare che in base al parametro della maggiore restrittività riservata dalla attuale disciplina è possibile identificare (almeno) una ulteriore tipologia di dati, segnatamente quelli relativi ai minori, in riferimento ai quali il GDPR segna un vero e proprio passo in avanti rispetto alla normativa previgente. In proposito, si veda: OROFINO M., *Minori e diritto alla protezione dei dati personali*, in OROFINO M., PIZZETTI F., *Privacy, Minori e cyberbullismo*, Giappichelli, Torino, 2018, pp. 1-30.

regolamento come tali, ma è presente un preciso riferimento al tipo di trattamento che permette di produrli.[31] L'articolo 4, al punto 5) chiarisce che la pseudonimizzazione coincide con quel tipo di processo diretto a garantire "che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile". Il trattamento in esame consiste dunque in un processo di de-identificazione eseguita per mezzo della sostituzione di un attributo contenuto in un dato personale con uno pseudonimo al fine di prevenire l'identificazione diretta dell'individuo cui, tuttavia, il dato continua a riferirsi. Dunque, a differenza del processo di anonimizzazione di cui si dirà in seguito, essa non mira a recidere in via definitiva la corrispondenza tra il dato personale e l'interessato. Al contrario, spesso l'applicazione della pseudonimizzazione presuppone la necessità per il titolare del trattamento di mantenere aperta la possibilità di ricostruire quel legame con certezza.[32] Proprio le "informazioni aggiuntive" richiamate dal GDPR costituiscono la chiave per mezzo della quale il titolare conserva la facoltà di

[31] Il termine "dati pseudonimizzati" viene utilizzato nel contesto del presente lavoro come espressione per descrivere con maggiore fluidità i dati sottoposti ad una procedura di pseudonimizzazione. Tuttavia, si segnala che il GDPR non definisce un'autonoma categoria di informazioni come dati pseudonimizzati.
Inoltre, è opportuno precisare che le considerazioni svolte sul tema valgono altresì per una tipologia di dati che, per certi versi, è assimilabile a quelli pseudonimizzati, ossia i dati cifrati. Malgrado si tratti di uno strumento in parte differente, l'articolo 32 del GDPR equipara la cifratura alla pseudonimizzazione, includendola tra le "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio".

[32] D'ACQUISTO G., NALDI M., *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, in *I diritti della "rete" nella rete*, Giappichelli, 2017, pp. 37-39.

individuare nuovamente l'attributo originale nascosto dietro a quello alterato.

Malgrado si tratti di un metodo di de-identificazione, la strutturale permanenza della possibilità da parte del titolare del trattamento di ricondurre un'informazione alla persona fisica porta a considerare detta persona come identificabile e, conseguentemente, a qualificare i dati sottoposti ad un processo di pseudonimizzazione come dati a carattere personale. Questa è la logica che informa il GDPR, [33] il quale all'inclusione di tali dati nel suo ambito di applicazione fa corrispondere l'inquadramento della pseudonimizzazione come misura tecnica ed organizzativa sia al fine di dare attuazione al principio di *privacy by design*,[34] sia allo scopo di garantire un livello di sicurezza adeguato contro i rischi di lesione per i diritti e le libertà degli individui.[35]

Per quanto riguarda il regime meno gravoso cui sottostanno i dati sottoposti a pseudonimizzazione, il GDPR non prevede nessuna disposizione esplicita di carattere eccezionale rispetto alla disciplina ordinaria come avviene, invece, per le ipotesi di categorie particolari di dati. Tuttavia, adottando lo stesso approccio orientato alla valutazione del rischio che caratterizza il regolamento, è possibile intravedere alcuni spiragli in cui i dati pseudonimizzati permettono al titolare del trattamento di fare ricorso a meccanismi derogatori. [36]

Ad esempio, l'implementazione di procedure di pseudonimizzazione costituisce uno dei fattori che potrebbero

[33] Un passaggio del cons. n. 26 recita: "I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile".
[34] Art. 25, par. 1, Regolamento (UE) 2016/679. In proposito, si rimanda a: D'ACQUISTO G., NALDI M., *Big data e privacy by design, op. cit*.
[35] Art. 32, par. 1, *lett*. a), Regolamento (UE) 2016/679.
[36] AGCM, AGCOM, Garante per la protezione dei dati personali, *Indagine conoscitiva sui big data*, 2018, *op. cit*., p. 64.

consentire di trattare i dati per una finalità ulteriore e differente rispetto a quella per cui sono stati originalmente raccolti, derogando in tal guisa al principio di limitazione delle finalità.[37] La medesima impostazione vale, *a fortiori*, per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nel contesto del quale la pseudonimizzazione viene identificata dall'articolo 89 come una fra le possibili misure tecniche ed organizzative a garanzia dei diritti e delle libertà dell'interessato utili ai fini della legittimazione di questa particolare tipologia di trattamento.

Ancora, il decremento del rischio derivante dall'applicazione dalla pseudonimizzazione dei dati personali svolge una funzione di irrobustimento della più delicata fra le basi giuridiche che consentono il trattamento: l'interesse legittimo del titolare o di terzi.[38] Il ricorso a tale criterio presuppone l'effettuazione di un preliminare "test comparativo" tra gli interessi del titolare del trattamento, o del terzo cui i dati vengono comunicati, e i diritti o gli interessi delle persone fisiche coinvolte. Tra i vari elementi che assumono rilievo nello svolgimento di tale bilanciamento ricorrono l'impatto che il trattamento in questione è in grado di produrre sulla sfera giuridica degli interessati e le correlative misure supplementari atte a mitigare tale impatto. Fra queste, la pseudonimizzazione gioca un ruolo chiave per far propendere l'ago della bilancia in favore dell'interesse del titolare: le ridotte possibilità di nocumento per l'individuo contribuiscono a legittimare le operazioni di elaborazione eseguite sui suoi dati personali.[39]

---

[37] Art. 6 par. 4, *lett*. e), Regolamento (UE) 2016/679.
[38] Art. 6 par. 1, *lett*. f), Regolamento (UE) 2016/679.
[39] Gruppo di lavoro articolo 29, "Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE" (WP 217), adottato il 9 aprile 2014, pp. 49-51.

Infine, ulteriori deroghe potrebbero scorgersi in tutte quelle ipotesi in cui il regolamento prevede una sorta di gradualità nella prescrizione degli oneri gravanti sul titolare in ragione del diverso livello di rischio sotteso al trattamento. Si pensi agli obblighi di notifica all'autorità di controllo o di comunicazione all'interessato nel caso di violazione di dati personali.[40] Nell'eventualità in cui ad essere violato sia solo il dataset di dati sottoposti ad una adeguata procedura di pseudonimizzazione, senza che le informazioni aggiuntive siano state carpite, il titolare può essere esentato dai suddetti doveri laddove il procedimento prescelto sia in grado di rendere il rischio per i diritti e le libertà delle persone fisiche improbabile, nel primo caso, oppure non elevato, nel secondo.

A completamento della disamina dei dati personali sottoposti a pseudonimizzazione, è doveroso riportare le ulteriori voci che propongono una concezione della fattispecie differente da quella che emerge dal testo del GDPR, specie alla luce della rilettura in chiave contestuale della qualificazione del dato che viene proposta nell'ambito della presente tesi. Tali critiche muovono dal presupposto che la definizione di pseudonimizzazione rinvenibile nell'articolo 4 del GDPR, laddove si riduce ad un'indicazione di risultato piuttosto che di una specifica procedura tecnica da seguire, differisca rispetto a quella convenzionalmente utilizzata. [41] Tale approccio si ispira ad una visione maggiormente pragmatica delle tecniche di de-identificazione che rinviene la chiave per individuare l'esatta natura dell'informazione non sulla definizione data dall'articolo 4, punto 5) del GDPR, quanto piuttosto su quell'inciso

[40] Artt. 33 e 34, Regolamento (UE) 2016/679.
[41] MOURBY M., MACKEY E., ELLIOT M., GOWANS H., WALLACE S., BELL J., SMITH H., AIDINLIS S., KAYE J., *Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the U*K, in *Computer Law & Security Review*, 2018, pp. 222 e ss.

del considerando n. 26 in cui si fa riferimento ai mezzi di cui il titolare del trattamento o un terzo possono ragionevolmente avvalersi per portare a termine con successo l'identificazione. [42] L'orientamento si colloca nel solco dell'impostazione promossa dallo Information Commissioner Office (ICO), l'autorità per la protezione dei dati britannica, ancor prima che il regolamento del 2016 vedesse la luce. Secondo l'ICO, la questione della pseudonimizzazione dovrebbe rimanere circoscritta al tema delle misure volte a garantire la sicurezza dei dati senza arrivare ad intaccare il profilo definitorio del dato personale, atteso che l'implementazione di una corretta procedura di pseudonimizzazione potrebbe anche produrre dati anonimi, ossia non personali, se le conseguenti difficoltà che si frappongono alla scoperta del dato originale dietro allo pseudonimo non possono essere superate tramite mezzi ragionevolmente utilizzabili. [43] Le problematiche interpretative individuate dall'autorità britannica derivano dalla tensione irrisolta presente nel considerando n. 26, tra l'assolutezza della qualificazione dei dati pseudonimizzati come personali e il relativismo dei mezzi che possono essere ragionevolmente utilizzati dal titolare del trattamento.[44] In tal senso, è evidente che già per i dati sottoposti a pseudonimizzazione si pone l'interrogativo relativo all'opportunità di un cambio di prospettiva, nella specie diretto ad una rilettura in chiave contestuale, per la qualificazione della natura delle informazioni.

Un'ulteriore categoria di dato che si pone in stretta continuità con quella dei dati pseudonimizzati è rappresentata dai dati definiti

[42] *Ibid.*
[43] INFORMATION COMMISSIONER OFFICE (ICO), *ICO analysis of the Council of the European Union text of the General Data Protection Regulation*, p. 2.
[44] *Ibid.*

dall'articolo 11 del GDPR. La disposizione disciplina i trattamenti le cui finalità non richiedono l'identificazione dell'interessato e, in un'ottica di incremento del livello di de-identificazione, esenta il titolare medesimo dalla conservazione o raccolta delle ulteriori informazioni necessarie a detta identificazione al solo fine di rispettare il regolamento.[45] Tuttavia, nel caso in cui il *data subject* decidesse di esercitare i diritti ad esso riconosciuti, potrebbe egli stesso fornire al titolare le informazioni aggiuntive mancanti.[46] L'elemento distintivo dei dati ex articolo 11 risiede nel fatto che le informazioni essenziali all'identificazione non sono in possesso né del titolare del trattamento, né di un terzo, come nell'ipotesi prevista dal considerando n. 26. Al contrario, è lo stesso interessato che le fornisce e che, pertanto, si identifica volontariamente.[47] Malgrado residuino dei dubbi sulla sua qualifica di categoria autonoma,[48] il maggiore rischio di identificabilità sotteso ai dati ex articolo 11 spinge la dottrina ad inserirli in una posizione intermedia tra i dati

[45] Art. 11, par. 1, Regolamento (UE) 2016/679.
[46] Art. 11, par. 2, Regolamento (UE) 2016/679.
[47] I casi in cui la dottrina ha riscontrato le circostanze di cui all'articolo in parola coincidono con quelle situazioni in cui il titolare del trattamento ha ricevuto dati pseudonimizzati senza però ottenere la chiave per la re-identificazione, oppure nelle ipotesi di pubblicazione di dataset ritenuti, a torto, anonimizzati. In tal senso, HINTZE M., *Viewing the GDPR through a De-Identification Lens: A Tool for Compliance, Clarification, and Consistency*, in *International Data Protection Law*, *Oxford University Press*, Vol. 8, Issue 1, 2018, pp. 86–101. Secondo l'A., rientrano in tale categoria i dati detenuti dal titolare che ha proceduto alla originaria pseudonimizzazione anche dopo che questi abbia distrutto le informazioni aggiuntive utili ad invertire il procedimento. Invero, tale conclusione non è scontata, atteso che, se risulta impossibile re-identificare gli interessati, i relativi dati potrebbero considerarsi non personali.
[48] Ad esempio, le "Linee guida sul diritto alla portabilità dei dati" elaborate dal Gruppo di lavoro articolo 29 sembrano considerare tali dati come pseudonimi e le disposizioni dell'art. 11 del GDPR come una norma di carattere pragmatico volta a facilitare l'esercizio dei diritti individuali in alcune ipotesi specifiche. A tale proposito, si veda: Gruppo di lavoro articolo 29 per la protezione dei dati, "Linee guida sul diritto alla portabilità dei dati" (WP 242), 2017, p. 10.

pseudonimizzati e quelli anonimizzati, anche alla luce della loro parziale sovrapponibilità.[49]

Infine, oltre a quelle che si evincono direttamente dal regolamento, sono possibili altre ed innumerevoli classificazioni delle informazioni che rientrano nella macrocategoria del dato personale a seconda del parametro di riferimento adottato dall'osservatore.[50] A tale riguardo, l'elaborazione di tassonomie volte a suddividere la categoria del dato personale in sottoinsiemi che presentano caratteristiche comuni non si esaurisce in un mero virtuosismo accademico. Al contrario, simile pratica è in grado di offrire un prezioso aiuto per avviare un dialogo comune e interdisciplinare in merito ad una eventuale riforma del *data law*.[51]

Fra le varie teorie che popolano il versante dottrinale, risulta meritevole di approfondimento quella proposta nel 2014 da Martin Abrams in ragione degli interrogativi concernenti il regime normativo applicabile ad alcune specifiche tipologie di

[49] RUNSHAN H., STALLA-BOURDILLON S., YANG M., SCHIAVO V. SASSONE V., *Bridging Policy, Regulation, and Practice? A Techno-Legal Analysis of Three Types of Data in the GDPR*, in LEENES R., VAN BRAKEL R., GUTWIRTH S., DE HERT P. (edited by), *Data Protection and Privacy: The Age of Intelligent Machines*, 2017, pp. 115 e ss.

[50] Le tassonomie di dati possono essere infinite e mai definitive. Ad esempio, l'Enterprivacy Consulting Group (cfr. Enterprivacy Consulting Group, Categories of Personal Information, 2017) ha tentato di fornire una panoramica generale e non esaustiva individuando sei diverse categorie di dati che attengono alla persona fisica (internal, historical, financial, external, social, tracking), ma chiarendo che la medesima informazione può appartenere simultaneamente a più categorie. Se si concentra l'analisi in uno specifico settore è possibile definire ulteriori sottocategorie di dati personali. Nel contesto dei social network, sono state delineate cinque differenti tipologie di dati (service, disclosed, entrusted, incidental, behavioral) disciplinati da differenti regole e gestiti in maniera diversa dai singoli titolari del trattamento (cfr. SCHNEIER B., *Schneier on Security, A blog covering security and security technology*, 2010). In alcuni casi, la classificazione dei dati arriva addirittura a prescindere, in parte, dalla distinzione tra personali e non personali: in un report del National Board of Trade svedese vengono elencate cinque categorie di dati (corporate, end-customer, human resources, merchant, technical) sulla base del loro utilizzo da parte delle imprese (cfr. National Board of Trade (Kommerskollegium), *No Transfer, No Trade: the Importance of Cross-Border Data Transfers for Companies Based in Sweden*, 2014).

[51] World Economic Forum, *Rethinking Personal Data: A New Lens for Strengthening Trust, Industry Agenda prepared in collaboration with A.T. Kearney*, 2014, p. 15.

informazioni.[52] La tassonomia in esame si fonda sul criterio dell'origine dei dati, ossia sulle modalità per mezzo delle quali essi vengono prodotti, e individua quattro differenti categorie.[53] La prima classe è rappresentata dai "*provided data*", quelli della cui generazione il *data subject* ha piena contezza avendovi partecipato attivamente e direttamente. La seconda categoria, quella degli "*observed data*", include le informazioni raccolte tramite attività di osservazione che, nell'era moderna, sono svolte da apparecchi elettronici in grado di monitorare costantemente e con elevato livello di dettaglio l'agire umano tanto nel mondo virtuale quanto in quello reale. In un momento cronologicamente successivo si colloca la generazione dei "*derived data*", ossia dei dati ricavati per mezzo di processi aritmetici o di correlazioni fra le informazioni già raccolte in precedenza. Similmente, l'ultima categoria degli "*inferred data*" è composta da dati dedotti da altri dati, che però, a differenza della tipologia precedente, si traducono in informazioni di carattere probabilistico in quanto, sulla base di processi statistici o di *Big Data analysis*, mirano ad anticipare i comportamenti o gli eventi relativi al *data subject*.[54]

Le ultime tre categorie elencate sono accomunate da due tendenze che sollevano interessanti questioni dal punto di vista giuridico. Da un lato, la digitalizzazione, l'*Internet of Things* e i *Big*

[52] La stessa tassonomia di Abrams trae spunto da un documento dal World Economic Forum che elenca tre tipologie di dati in base al modo in cui vengono raccolti. Il medesimo documento ipotizzava un'ulteriore categorizzazione dei dati personali che suddivideva le differenti informazioni disponibili nel mondo digitale (Digital identity, Relationships to other people and organisations, Real-world and online context, activity, interests and behaviour, Communications data and logs, Media produced, consumed and shared, Financial data, Health data, Institutional data). A tale riguardo, si veda: World Economic Forum, *Personal Data: The Emergence of a New Asset Class, An Initiative of the World Economic Forum In Collaboration with Bain & Company, Inc.*, 2011, pp. 13-15.
[53] ABRAMS M., *The Origins of Personal Data and its Implications for Governance*, The Information Accountability Foundation, 2014.
[54] *Ibid*. pp. 6-8.

Data stanno portando ad un aumento esponenziale di questi dati con la conseguente riduzione della quantità di dati forniti direttamente dall'interessato. Dall'altro lato, i dati *observed, derived* e *inferred* si caratterizzano tutti per un livello di consapevolezza dell'interessato in merito alla loro generazione e successiva elaborazione piuttosto basso.[55] Dunque, ci stiamo avviando verso – *rectius*, ci troviamo già in – uno scenario in cui la maggioranza dei dati personali in circolazione sono trattati senza che gli individui cui quei dati si riferiscono ne siano pienamente al corrente.

In tale prospettiva è lecito domandarsi se la definizione di dato personale del regolamento europeo comprenda tutte le categorie di dati appena elencati e, pertanto, prescriva le stesse regole per tutti i titolari del trattamento indipendente dal tipo di dati gestiti. Se si muove dal presupposto che la protezione dei dati personali rientra fra i diritti fondamentali dell'ordinamento continentale, la risposta più ovvia dovrebbe essere affermativa, in quanto non vi sarebbe alcun motivo per limitare l'esercizio di un diritto fondamentale in ragione delle modalità di produzione dell'informazione. A ben vedere, in un'ottica di tutela effettiva, le regole sul trattamento dei dati dovrebbero trovare applicazione, *a fortiori*, in un contesto in cui i processi di generazione ed elaborazione dei dati si collocano ad una distanza maggiore dall'individuo da proteggere.[56]

Tuttavia, nell'unica disposizione del GDPR in cui è rinvenibile un'indicazione che sembra dare rilievo ad una tassonomia basata sull'origine dei dati, il legislatore si è mosso in direzione opposta. L'articolo 20, concernente il diritto alla portabilità,[57]

[55] *Ibid*. pp. 3-4.
[56] World Economic Forum, *Rethinking Personal Data*, *op. cit.* pp. 15-16.
[57] Come si evince dal primo paragrafo dell'art. 20 del GDPR, tale diritto consiste nella facoltà per l'interessato "di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento

include uno specifico riferimento ai dati forniti (*provided*) dall'interessato e circoscrive l'esercizio del relativo diritto solo a questa tipologia di dati personali. A chiarire eventuali dubbi in merito alla portata interpretativa di tale passaggio sono intervenute le linee guida sul diritto alla portabilità dei dati elaborate dal Gruppo di lavoro articolo 29, nelle quali siffatta limitazione viene illustrata in maniera puntuale.[58] Il documento conferma che l'esercizio del diritto in parola deve essere circoscritto ai dati forniti dall'interessato, aggiungendo, tuttavia, che devono considerarsi parte di tale categoria anche i dati derivanti dalla osservazione delle attività dell'interessato, dunque, quelli che Abrams ha definito *observed data*. Nel prosieguo, il Gruppo richiama, alla lettera, le tipologie di informazioni *derived* e *inferred* e le esclude dal novero dei dati per cui il *data subject* può richiedere la trasmissione.[59]

Orbene, malgrado la lettura proposta dal Gruppo di lavoro susciti qualche perplessità, essa non implica necessariamente che tutti i diritti riconosciuti agli interessati, o addirittura l'intero impianto normativo del GDPR, siano circoscritti ai dati forniti od osservati. Lo stesso documento precisa, fra l'altro, che il diritto all'accesso a tali dati rimane immune alla classificazione basata sulla loro origine,[60] tenendo pertanto a distanza la portabilità che, fra tutti

---

e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti".

[58] Gruppo di lavoro articolo 29, "Linee guida sul diritto alla portabilità dei dati", *op. cit.*, pp. 10-12.

[59] Nella versione inglese delle Linee guida, vengono utilizzati gli stessi termini della tassonomia di Abrams.

[60] *Ibid*. p. 11, dove, in nota, il Gruppo di lavoro afferma che: "l'interessato può sempre esercitare il "diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali" nonché informazioni riguardanti "l'esistenza di decisioni automatizzate, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato", in base all'articolo 15 del RGPD (relativo al diritto di accesso)".

i diritti riconosciuti alla persona, risulta essere quello più condizionato.[61] Tuttavia, sorge spontanea la domanda in merito ai motivi che si celano dietro alla decisione di optare per una soluzione simile e, soprattutto, se questo tipo di differenziazione riuscirà a trovare spazio anche con riferimento ad altri istituti previsti dal regolamento sui dati personali. La questione si pone in maniera particolarmente pressante con riguardo agli *inferred data*, in quanto la loro produzione richiede ingenti investimenti da parte di imprese o istituzioni che, in ragione dell'elevato potenziale derivante dal carattere predittivo, sono disposte a tenerseli stretti anche facendo ricorso a meccanismi di protezione della proprietà intellettuale.[62] Basti pensare al diritto di rettifica riconosciuto dall'articolo 16 del GDPR. In che misura sarà consentito chiedere e ottenere la rettifica del dato dedotto da algoritmi utilizzati, ad esempio, da compagnie assicurative o istituti di credito sulla base del quale viene fondato il diniego all'accesso a determinati servizi o benefici? Il titolare del trattamento potrà impedire all'interessato di contestare la veridicità di quel dato in quanto non raccolto ma creato attraverso strumenti di proprietà dell'azienda?

In definitiva, le tassonomie interne alla categoria del dato personale, non assumendo carattere puramente descrittivo, si rivelano fondamentali al fine di individuare i punti deboli della disciplina nell'intento di stimolare discussioni giuridiche con enormi risvolti pratici. Lo sviluppo delle tecnologie di data *analytics*, *machine learning* e *Big Data* sta palesando nuove istanze di protezione per interessati che si trovano in balìa di modalità di

[61] Sempre l'art. 20 consente l'esercizio di tale diritto solo nelle ipotesi in cui: a) il trattamento sia basato sul consenso o su un contratto e b) il trattamento sia effettuato con mezzi automatizzati.
[62] World Economic Forum, *Rethinking Personal Data*, *op. cit.* pp. 15-16.

trattamento dei propri dati sempre più oscure e lontane dalla loro conoscenza, mettendo pertanto a repentaglio la possibilità di autodeterminarsi liberamente e autonomamente. Queste e altre questioni necessiteranno in futuro di adeguato approfondimento, specie alla luce di un regolamento, il GDPR, che si dimostra particolarmente attento al versante della raccolta dei dati, ma che rischia di mostrare il fianco quando i dati, come quelli *derived* e *inferred*, non vengono raccolti, bensì prodotti dal titolare del trattamento.[63]

2.2 Gli elementi costitutivi del dato personale

La comprensione della fattispecie del dato a carattere personale passa attraverso l'analisi dei quattro elementi che compongono la definizione normativa: "qualsiasi informazione", "riguardante", "persona fisica", "identificata o identificabile". Un'informazione può considerarsi personale solamente se presenta simultaneamente queste quattro caratteristiche. L'esame delle singole componenti svolta nei paragrafi successivi assumerà quale punto di riferimento uno fra i più autorevoli documenti in tema di definizione di dato personale adottato dal Gruppo di lavoro articolo 29 che nel 2007 ha pubblicato il suo "Parere 4/2007 sul concetto di dati personali".[64]

Sebbene concepito nel contesto della disciplina precedente e, apparentemente, superato per l'epoca digitale, la mancanza di modifiche significative con riguardo al nucleo della definizione di dato personale rende il Parere ancora una valida base di partenza per

[63] ABRAMS M., *The Origins of Personal Data and its Implications for Governance*, *op. cit.*, pp. 9-11.
[64] Gruppo di lavoro articolo 29 per la protezione dei dati personali, "*Parere 4/2007 sul concetto di dati personali*" (WP136).

una approfondita disamina delle problematiche che affliggono il quadro regolamentare attualmente vigente. Per di più, il dichiarato obiettivo di fornire una interpretazione univoca del concetto di dato personale alla luce delle differenti prassi applicative riscontrate negli Stati membri, ha fatto sì che anche la giurisprudenza della Corte di giustizia fondasse i suoi orientamenti proprio sulle indicazioni fornite dal Gruppo di lavoro.[65]

a) Qualsiasi informazione

L'inciso "qualsiasi informazione" rende sin dal principio manifesta l'ampiezza della nozione di dato personale. Innanzitutto, tradurre la parola "dato" con "informazione" riflette una precisa scelta metodologica da parte del legislatore europeo: l'utilizzo promiscuo di entrambi i termini, senza circoscriverli all'interno del perimetro tecnico che solitamente compete loro, deriva dalla volontà di introdurre una nozione tecnologicamente neutra e, conseguentemente, tecnologicamente adattabile. Infatti, nel settore dell'informatica, il dato rappresenta il vettore che trasporta l'informazione, la quale, a sua volta, coincide con il contenuto semantico, ossia il significato, che viene attribuito a quel dato.[66] L'utilizzo di una terminologia piuttosto generica e, in un certo senso, a-tecnica rappresenta una costante delle più recenti prassi legislative, che spesso hanno soprasseduto sulla necessità di approfondire i profili definitori del settore dell'*Information and Communication*

[65] Sul ruolo e sull'influenza del Gruppo di lavoro articolo 29, si veda: POULLET Y., GUTWIRTH S., *The contribution of the Article 29 Working Party to the construction of a harmonised European dataprotection system: an illustration of 'reflexive governance'?* in PEREZ ASINARI M. V., PALAZZI P. (Eds) *Défis du droit à la protection de la vie privée. Challenges of privacy and data protection law - Challenges of privacy and data protection law*, 2008, pp. 570 e ss.

[66] L'accezione tecnica e circoscritta al significato sintattico del termine "data" è fornita dallo standard ISO/IEC 2382:2015 che lo definisce: "reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing".

Technology, in quanto operazione ritenuta superflua e di scarsa utilità pratica.[67] Sebbene simile atteggiamento sia criticabile a causa degli effetti indesiderati che ne potrebbero derivare, specie quello di "*over-inclusiveness*", ossia di eccessivo allargamento dell'ambito di applicazione della legge,[68] tale questione sembra pesare in misura minore con riguardo al GDPR. Per un regolamento che si pone come obiettivo quello di ricomprendere la maggior parte delle informazioni in circolazione in territorio europeo, quando legate ad una persona fisica, il rischio di smisurato allargamento del campo applicativo non deriva tanto dall'elemento informazione, quanto, piuttosto, da quello della identificabilità.[69]

La genericità del primo elemento si traduce, ad opinione del Gruppo di lavoro, in tre aspetti principali. Innanzitutto, vengono ricomprese informazioni di qualsiasi natura, tanto oggettive, ossia ontologicamente verificabili, quanto soggettive, poiché espressione di un punto di vista individuale. La presenza di dati di natura soggettiva implica che la qualifica di dato personale spetta anche alle informazioni false. La mancanza di aderenza alla realtà non recide il legame di un dato con il *data subject* e, pertanto, non può giustificare il diniego di un diritto riconosciutogli dal GDPR. Del resto, il diritto di rettifica e, in parte, il diritto di limitazione del trattamento identificano la supposta erroneità dei dati trattati quale condizione legittimante il loro esercizio.[70]

Ad ogni modo, la possibilità di contestare l'erroneità di dati soggettivi, che in quanto tali rimangono opinabili, risulta

[67] BYGRAVE L., *Information Concepts in Law: Generic Dreams and Definitional Daylight*, in *Oxford Journal of Legal Studies*, Vol. 35, No. 1, 2015, pp. 91 e ss.
[68] *Ibid*. pp. 91-95.
[69] COLAPIETRO C., *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale, op. cit.*, pp. 13-19.
[70] Art. 16 e art. 18, par. 1, lett. a), Regolamento (UE) 2016/679.

naturalmente più ridotta rispetto alle ipotesi in cui l'errore è oggettivamente dimostrabile. La Corte di giustizia, nella sentenza *Nowak*, dopo aver stabilito che la valutazione espressa da un esaminatore in sede di prova equivale a dato personale concernente l'esaminato, ha circoscritto le facoltà di esercizio del diritto di rettifica ai soli casi di errori grossolani,[71] giacché tale diritto "non può, evidentemente, consentire al candidato di «rettificare», a posteriori, risposte «sbagliate»".[72] Tuttavia, rispetto all'epoca in cui il Gruppo di lavoro ha pubblicato il suo parere, l'inserimento della componente artificiale – la "macchina" – nei procedimenti decisionali ha amplificato enormemente le problematiche inerenti ai dati soggettivi. La possibilità di confutare la validità di una valutazione prodotta da un algoritmo rischia di assottigliarsi a seguito del nuovo approccio metodologico promosso dalla tecnologia *Big Data*.[73] Sebbene abbia consentito di individuare *pattern* che solitamente sfuggono alle capacità computazionali finora conosciute, essa ha al contempo offuscato le logiche che guidano la decisione algoritmica.[74] Di conseguenza, la posizione dell'interessato ne esce

[71] Corte di Giustizia, causa C-434/16, Nowak, *cit*. In particolare, la Corte riconosce la facoltà per un candidato a un esame di ottenere la rettifica delle annotazioni dell'esaminatore relative alle risposte fornite in occasione di una prova scritta in situazioni nelle quali le valutazioni siano inesatte "per esempio per il fatto che, per errore, le prove di esame sono state scambiate in modo tale che le risposte di un altro candidato siano state attribuite al candidato interessato, o che una parte dei fogli contenenti le risposte di tale candidato è stata smarrita con la conseguenza che tali risposte sono incomplete o, ancora, che le eventuali annotazioni dell'esaminatore non documentano correttamente la valutazione da esso effettuata delle risposte del candidato interessato", (par. 54).

[72] *Ibid*., par. 52.

[73] SIMONCINI A., SUWEIS S., *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, Fascicolo 1, *2019, pp. 87-106.*

[74] Sul tema della tensione tra decisioni algoritmiche e GDPR, con particolare riguardo al cd. *right to explanation*, si veda: BRKAN M., BONNET G., *Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas*, in *European Journal of Risk Regulation*, Vol. 11, Issue 1, 2020, pp. 18 e ss.

piuttosto indebolita,[75] specie di fronte a quei dati di carattere predittivo che rispecchiano solamente una analisi statistica diretta a stabilire la probabilità del verificarsi di determinati scenari.[76]

Gli altri due aspetti coinvolti nell'ambito del primo elemento della definizione di dato personale riguardano il contenuto e la forma. In merito al profilo contenutistico, il Gruppo di lavoro sottolinea *expressis verbis* che le varie dimensioni della vita del *data subject* e le differenti sottocategorie – esaminate in precedenza – cui possono appartenere le informazioni non intaccano la natura del dato che rimane comunque personale.[77]

Inoltre, con riguardo al formato in cui l'informazione deve essere veicolata, le precisazioni presenti sembrano frutto, essenzialmente, del tempo in cui la Direttiva Madre era stata approvata.[78] L'avvertita necessità da parte del Gruppo di lavoro di ribadire che, fra l'altro, suoni ed immagini vanno annoverati nel catalogo dei dati suscettibili, al ricorrere di tutti gli altri elementi, di divenire personali fa da eco ai timori che erano stati espressi dal legislatore stesso nel testo della direttiva.[79] Peraltro, attualmente,

---

[75] Di vero e proprio "potere dell'algoritmo" parla: GARZONIO E., *L'algoritmo trasparente: obiettivi ed implicazioni della riforma dello Spazio digitale europeo*, in *Rivista italiana di informatica e diritto*, fasc. n. 2/2021, pp. 25 e ss.

[76] Sui rimedi esperibili dall'individuo destinatario di una decisione algoritmica, si veda: NOTO LA DIEGA G., *Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (JIPITEC), 2018, pp. 3-34.

[77] Gruppo di lavoro articolo 29, "*Parere 4/2007 sul concetto di dati personali*", op. cit., p. 7.

[78] *Ibid.*, p. 8.

[79] Oltre al considerando n. 14, la Direttiva 95/46/CE dedicava una disposizione specifica dell'art. 33 a tale tema: "La Commissione presenta periodicamente al Consiglio e al Parlamento europeo, per la prima volta entro tre anni dalla data di cui all'articolo 32, paragrafo 1, una relazione sull'applicazione della presente direttiva, accompagnata, se del caso, dalle opportune proposte di modifica. La relazione è oggetto di pubblicazione.
La Commissione esaminerà in particolare l'applicazione della presente direttiva al trattamento dei dati sotto forma di suoni o immagini relativi a persone fisiche e presenterà le eventuali proposte necessarie, tenuto conto dell'evoluzione della tecnologia dell'informazione e alla luce dei progressi della società dell'informazione".

l'assenza dei medesimi riferimenti nel GDPR lascia presumere che, nell'era della datificazione, le questioni relative al formato possano considerarsi definitivamente superate.

b) Concernente (o riguardante)

L'elemento consistente nell'inciso "concernente" nella versione della Direttiva Madre, o "riguardante" in quella del GDPR – mentre il "relating to" della versione inglese è rimasto inalterato in entrambi i provvedimenti normativi – esalta il collegamento che deve sussistere tra la persona fisica e il dato affinché questo possa essere considerato personale.

Al di là dell'ipotesi elementare in cui sussiste un collegamento diretto con l'interessato, è ben possibile considerare come personale anche un dato riferito in via principale ad un oggetto laddove questo riesca al contempo a rivelare informazioni riguardanti una persona fisica determinata.[80] A tale proposito, ambiti quali l'*Internet of Things*, la domotica o la *smart manufacturing*, su cui si focalizzano gran parte degli sviluppi tecnologici più recenti, rappresentano contesti in cui tale evenienza si verifica frequentemente, poiché la perpetua e indiscriminata raccolta di dati effettuata dai sensori integrati nei macchinari intelligenti potrebbe comportare l'acquisizione di informazioni relative a svariate persone fisiche, lavoratori compresi.[81]

---

[80] Gruppo di lavoro articolo 29, "*Parere 4/2007 sul concetto di dati personali*", *op. cit*., pp. 9-10.

[81] Ad esempio, i dati relativi alla quantità giornaliera di beni di consumo realizzati nel contesto di un determinato processo produttivo possono contenere informazioni relative alle capacità lavorative dell'operaio che interviene in una delle fasi del processo di produzione. Informazioni che poi entreranno nella disponibilità dal datore di lavoro, con tutto ciò che ne consegue in termini di gestione del rapporto di lavoro. Per un approfondimento sul tema della tutela dei lavoratori rispetto all'utilizzo delle tecnologie digitali, si veda: COLAPIETRO C., *Tutela della dignità e della riservatezza del lavoratore nell'uso delle tecnologie digitali per finalità di lavoro*, in *Giornale di diritto del lavoro e di relazioni industriali*, Franco Angeli, Milano, 2017, pp. 581-613.

Per scoprire se sussiste questo legame tra dato ed individuo, il Gruppo di lavoro propone di scindere l'inciso "concernente" in tre ulteriori elementi tra loro alternativi: uno di contenuto, uno di finalità e l'ultimo di risultato.[82] La prima componente non solleva particolari problematiche poiché si riferisce a quelle ipotesi in cui il dato vanta un legame diretto ed evidente con l'individuo. Il dato viene raccolto e trattato nella piena consapevolezza che le informazioni in esso contenute sono riferite ed una persona fisica. Di gran lunga più interessanti si rivelano, invece, le altre due componenti.

L'elemento di "finalità" evoca il fattore teleologico nella qualificazione del dato. Indipendentemente dal contenuto e dalla possibilità di ricondurlo direttamente ad una persona fisica, si rientra nella categoria personale "quando i dati sono usati o lo saranno probabilmente, tenendo conto di tutte le circostanze del caso di specie, al fine di valutare, trattare in un dato modo o influire sullo stato o sul comportamento di una persona".[83] Con tale espressione il Gruppo aggiunge un elemento probabilistico che impone una valutazione proiettata verso il trattamento futuro. L'informazione deve essere considerata come personale sin dal principio se le circostanze particolari del caso concreto lasciano presumere che, prima o poi, il titolare del trattamento deciderà di utilizzarla allo scopo di addivenire all'identificazione di un individuo; anche se, inizialmente, non vi era né l'intenzione, né la possibilità di realizzarla con successo. Questo orientamento non appare condivisibile nella misura in cui intende la natura del dato come fattore immutabile per l'intero ciclo di trattamento. Le modalità di elaborazione dei dati attuali richiedono un approccio maggiormente

[82] Gruppo di lavoro articolo 29, "*Parere 4/2007 sul concetto di dati personali*", *op. cit*., pp. 9-12.
[83] *Ibid*., pp. 10-11.

dinamico in grado di accogliere la costante variabilità della natura delle informazioni, le quali vanno considerate personali solamente per quei segmenti del trattamento in cui vengono elaborate per finalità identificative.[84] D'altro canto, è comunque doveroso precisare che simile concezione non può includere i trattamenti ontologicamente diretti ad individuare persone fisiche, come avviene nel caso della videosorveglianza. Sebbene le autorità pubbliche non procedano al riconoscimento di ogni singolo soggetto inquadrato, lo scopo del trattamento rimane quello di risalire all'identità di un determinato individuo nell'eventualità in cui si verifichino degli illeciti. Pertanto, i dati raccolti dalla telecamera rimarranno sempre di carattere personale.

Una complessità persino maggiore sembra contraddistinguere il terzo ed ultimo elemento elencato dal Gruppo di lavoro, quello del risultato. In tesi, la qualifica di dato personale emerge in tutte le ipotesi in cui, malgrado non ricorrano né la componente del contenuto, né quella di finalità, il trattamento dell'informazione è suscettibile di produrre un impatto sui diritti e sugli interessi di una persona fisica. Il rilievo di tale impatto non deve necessariamente essere di livello significativo, poiché viene ritenuto sufficiente un utilizzo del dato tale da comportare un trattamento diverso dell'individuo cui si riferisce.[85] Dunque, nel tentativo di tracciare una distinzione tra la componente della finalità da quella del risultato, è possibile ritenere che mentre nella prima ipotesi il trattamento miri principalmente ad incidere sulla sfera giuridica del *data subject*, nel secondo quest'effetto si presenta come eventuale e

[84] DALLA CORTE L., *Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protecton Law*, in *European Journal of Law and Technology*, Vol. 10, No. 1, 2019, pp. 11-12.
[85] Gruppo di lavoro articolo 29, "*Parere 4/2007 sul concetto di dati personali*", *op. cit*., p. 11.

ancillare rispetto all'utilizzo primario del dato. In un certo senso, per valutare la sussistenza della personalità del dato "per finalità" è opportuno adottare il punto di vista del titolare del trattamento, mentre nella personalità "per risultato", la prospettiva è quella della persona fisica, segnatamente del modo in cui questa percepisce quel tipo di trattamento.[86]

Questo è l'elemento che sconta maggiori difficoltà di conciliazione con la realtà di elaborazione di dati dell'epoca corrente. È possibile sostenere che nel mondo dei *Big Data* e delle *smart cities* esista ancora un trattamento di dati, di qualsiasi natura, che non sia suscettibile di avere un impatto sulla sfera giuridica di una persona fisica? In effetti, se si considera il contesto *data-intensive* verso il quale ci stiamo dirigendo, la prospettazione di uno scenario in cui tutte le informazioni in circolazione in ambiente digitale rientrano nella categoria di dato personale non appare un'ipotesi affatto speciosa.[87] I dati relativi alle condizioni della strada, al meteo e ai movimenti dei veicoli analizzati dagli algoritmi incorporati nelle automobili a guida autonoma oppure il calcolo delle quantità di prodotti da utilizzare nell'agricoltura di precisione sono esempi di informazioni di natura essenzialmente non personale la cui elaborazione può produrre un impatto, anche significativo, sulla sfera individuale.[88] Del resto, lo stesso concetto di *smart city* – o, ancor

[86] Il documento del Gruppo di lavoro riporta un esempio di un sistema di localizzazione delle vetture dei tassisti. Sebbene il sistema sia stato realizzato al fine di individuare la vettura più vicina a chi richiede il servizio, gli operatori potrebbero comunque comportarsi differentemente dal momento che i sensori di localizzazione permettono, potenzialmente, di valutare la loro prestazione.

[87] PURTOVA N., *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, in *Law, Innovation and Technology*, Vol. 10, No. 1, 2018, pp. 40 e ss.

[88] BRKAN M., BONNET G., *Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions*, *op. cit.*

più, quello di *smart landscape* –[89] presuppone la raccolta e l'analisi di tutte le informazioni ricavabili dall'ambiente circostante al preciso scopo di adattare quest'ultimo alle esigenze dei suoi cittadini e, dunque, producendo un impatto sugli stessi.[90]

Pertanto, gli elementi di finalità e risultato che, insieme a quello di contenuto, costituiscono condizioni alternative al ricorrere delle quali un dato può considerarsi personale, rischiano di creare una iperestensione della categoria in esame e, di conseguenza, dell'ambito di applicazione della disciplina in materia di protezione dei dati personali. Oltretutto, è opportuno notare che la costruzione tripartita del collegamento tra l'informazione e la persona fisica concepita dal Gruppo di lavoro non viene supportata da alcun riferimento normativo, in quanto non ve ne è traccia nella Direttiva Madre, e nemmeno nel GDPR. Ciononostante, la Corte di giustizia sembra comunque farla propria nella citata sentenza *Nowak*. In tale occasione, infatti, quando i giudici sono chiamati a pronunciarsi sulla portata del termine "concernente", affermano che tale elemento ricorre "qualora, in ragione del suo contenuto, della sua finalità o del suo effetto, l'informazione sia connessa a una determinata persona",[91] citando di fatto, quasi alla lettera, il parere sul concetto dei dati personali.

Tuttavia, l'avanzamento delle scienze tecnologiche rischia di condannare all'obsolescenza l'interpretazione fornita dal Gruppo di lavoro e seguita dalla Corte di giustizia. Infatti, in un'ottica di

[89] PAGNANELLI V., *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in *Rivista italiana di informatica e diritto*, fasc. n. 1/2021, pp. 14-15. L'A. descrive la nozione di *smart landscape* come un concetto più ampio della *smart city*, nella misura in cui individua come destinatari dei propri servizi e benefici non solo i cittadini, bensì anche le imprese e l'industria in genere, specie il settore della logistica per la circolazione delle merci.
[90] PURTOVA N., *The Law of Everything*, *op. cit.*
[91] Corte di Giustizia, causa C-434/16, Nowak, *cit.*, par. 35.

responsabilizzazione del titolare orientata alla valutazione sistematica e di contesto del rischio per l'interessato, diviene praticamente impossibile escludere l'identificabilità del *data subject* sulla base dell'applicazione dei criteri citati. L'esigenza di dare certezza alle regole che i titolari del trattamento devono seguire spinge verso una rilettura del secondo elemento della definizione che sia capace di disinnescare l'indefinita espansione della nozione di dato personale e di circoscrivere l'applicazione della disciplina alle sole eventualità in cui possa concretizzarsi un pericolo di lesione dei diritti degli individui.[92]

c) Persona fisica

La limitazione dell'applicabilità della disciplina solamente agli individui deriva dall'impiego del termine "persona fisica". Nonostante sia l'elemento che più degli altri contribuisce a circoscrivere la nozione di dato personale,[93] anche in questo caso le parole del Gruppo di lavoro restituiscono una esegesi piuttosto ampia. In ossequio al tratto distintivo del sistema continentale, la protezione assicurata dal quadro normativo europeo viene concepita

[92] DALLA CORTE L., *Scoping Personal Data*, *op. cit*.

[93] A tal proposito, è opportuno segnalare che l'utilizzo del genere singolare per l'elemento della persona fisica sembra escludere che il diritto alla protezione dei dati personali possa trovare pari tutela anche in riferimento agli interessi di gruppo. Tuttavia, non mancano in dottrina istanze tese a identificare la dimensione collettiva come la migliore modalità per una effettiva protezione dei dati personali nell'epoca corrente. A tale proposito si veda: 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*, 2016, pp. 238-255; MANTELERO A., *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era*, in TAYLOR L., FLORIDI L., VAN DER SLOOT B. (eds), *Group Privacy New Challenges of Data Technologies*, Springer, 2017, pp. 139-158.

come diritto universale,[94] escludendo la rilevanza di requisiti quali la cittadinanza e la residenza nel territorio dell'Unione.[95]

Simile impostazione risulta confermata nella sentenza *Schrems I*, in occasione della quale la Corte di giustizia ha motivato l'invalidazione della decisione con cui la Commissione aveva conferito idoneità al "*Safe Harbour*" sulla base, fra l'altro, della disparità di trattamento rimediale tra i cittadini statunitensi e quelli europei.[96] Il sistema americano ha nei fatti dimostrato di fondare la propria disciplina sulla separazione tra i cittadini – ai quali vengono equiparati i residenti permanenti – da un lato, e gli stranieri, dall'altro. Lo schermo protettivo fornito dalle disposizioni costituzionali forma un valido meccanismo di difesa delle ingerenze del potere pubblico nella sfera privata individuale solamente per chi ha sviluppato un legame sufficientemente forte con la comunità nazionale, ma non per quegli interessati residenti all'estero i cui dati sono stati trasferiti nei *server* di compagnie private che hanno la sede principale negli USA.[97]

Dunque, anche il confronto con l'ordinamento nordamericano dimostra il carattere ampiamente inclusivo della definizione presente nella legislazione europea,[98] la quale rifugge qualsiasi prospettiva di

---

[94] Gruppo di lavoro articolo 29, "*Parere 4/2007 sul concetto di dati personali*", *op. cit.*, p. 22. In particolare, il documento richiama l'art. 6 della Dichiarazione universale dei diritti umani che recita: "Ogni individuo ha diritto, in ogni luogo, al riconoscimento della sua personalità giuridica".

[95] Aspetto questo evidenziato anche dai considerando n. 2 e n. 14 del Regolamento (UE) 2016/679.

[96] Corte di Giustizia, 6-10-2015, causa C-362-14, Maximilian Schrems *c*. Data Protection Commissioner, par. 90.

[97] RESTA G., *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in RESTA, ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Collana "Consumatori e Mercato", 2016, pp. 23 e ss.

[98] Tra l'altro, è opportuno notare che le discrepanze tra gli ordinamenti europeo e statunitense in materia di dati derivano anche dal differente presupposto applicativo della normativa, laddove alla nozione di "dato personale" europea fa da contraltare quella statunitense di

tutela localizzata, per abbracciare, invece, un approccio protettivo valevole per tutti gli interessati i cui dati vengono generati o trasferiti nel territorio del vecchio continente.[99]

Per contro, la decisione di accordare la tutela esclusivamente alle persone fisiche, pone al di fuori dell'ambito di applicazione le informazioni concernenti le persone giuridiche. Le aperture mostrate dal legislatore europeo nelle direttive adottate negli anni Novanta e Duemila, [100] verosimilmente dettate dalla volontà di aggirare le difficoltà di distinzione personale-non personale in via "soggettiva", non sono state riprese con il GDPR, nel quale non compare alcuna facoltà espressa di estensione delle regole in materia di protezione di dati personali alle informazioni relative a soggetti di diritto diversi dalle persone fisiche. Cionondimeno, rimangono valide anche nel contesto del regime corrente le osservazioni svolte dal Gruppo in merito all'eventualità che, in circostanze particolari, anche le informazioni riguardanti persone giuridiche possano essere attirate al di sotto dell'ombrello del regolamento del 2016.[101] Il caso è quello relativo ai dati che, pur riferiti primariamente ad una persona giuridica, siano in grado di svelare informazioni riguardanti

"Personal Identifiabile Information". Sul punto, si veda: DUCATO R., *La crisi della definizione di dato personale nell'era del web 3.0, op. cit.*, pp. 143 e ss.

[99] L'art. 3 del GDPR, dedicato alla definizione dell'ambito di applicazione della disciplina, prescrive il rispetto dei relativi obblighi per il trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione (par. 1); ed 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 ivi stabilito, quando le attività di trattamento riguardano l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato, oppure il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione (par. 2).

[100] *Supra*, cap. I, par. 4.

[101] Gruppo di lavoro articolo 29, "*Parere 4/2007 sul concetto di dati personali*", *op. cit*., p. 23-24.

determinati individui:[102] in tale ipotesi, i dati devono essere trattati nel rispetto della disciplina in materia di protezione delle informazioni concernenti le persone fisiche.

Peraltro, non è corretto interdire integralmente le istanze legislative nazionali volte ad allargare la protezione accordata dal GDPR anche a dati diversi da quelli relativi alle persone fisiche. Su tale aspetto si era già espressa la Corte di giustizia che, in merito all'applicabilità della Direttiva Madre, aveva affermato che "nulla impedisce che uno Stato membro estenda la portata della normativa nazionale di attuazione della direttiva 95/46/CE a settori non compresi nell'ambito di applicazione di quest'ultima, purché non vi osti alcun'altra disposizione del diritto comunitario".[103]

In proposito, risulta interessante analizzare la scelta compiuta dal legislatore italiano che, tanto nel 1996, quanto nel 2003 in sede di modifica, aveva approfittato del margine di manovra garantito dalla direttiva. Agli esordi, l'articolo 4, comma 1, del Codice privacy ricomprendeva le persone giuridiche fra i soggetti beneficiari della tutela nel momento in cui definiva, alla lettera b), il dato personale come "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale" e, alla lettera i), l'interessato come "la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali". Solo con la riforma introdotta dall'articolo 40, comma 2 del decreto-legge 6

[102] Riprendendo le parole del documento: "È quel che accade quando il nome di una persona giuridica deriva dal nome di una persona fisica, oppure nel caso dell'indirizzo e-mail di un'impresa di norma usato da un dato dipendente, o delle informazioni su una piccola impresa (giuridicamente un "oggetto" piuttosto che una persona giuridica) che possono descrivere il comportamento del suo titolare".
[103] Corte di Giustizia, 6-11-2003, causa C-101/01, Lindqvist, par. 98.

dicembre 2011, n. 201, convertito con modificazioni dalla legge 22 dicembre 2011, n. 214, verrà soppresso qualsiasi riferimento alle persone giuridiche. La modifica in esame, introdotta al fine di ridurre gli oneri di *compliance* gravanti sui titolari del trattamento, ha però causato alcune incongruenze nel sistema che si era consolidato nel contesto nazionale. Anche il Garante italiano in un parere in cui individua una residua area di applicabilità del Codice privacy – nello specifico, il capo I del titolo X –[104] anche ai dati delle persone giuridiche, lamenta alcune carenze di coordinamento, prodottesi a seguito della riforma del 2011, tali da richiedere ulteriori valutazioni da parte del Parlamento e del Governo.[105] Pertanto, alla luce delle – pur limitate – ipotesi di potenziale applicazione, non risulta opportuno escludere *a priori* le informazioni attinenti alle persone giuridiche dall'ambito di interesse della disciplina, poiché si rivela comunque necessaria una attenta analisi delle implicazioni derivanti dal tipo trattamento che si sta eseguendo.

Un ultimo profilo meritevole di attenzione concerne la distinzione tra persone fisiche viventi e persone fisiche decedute. Il GDPR, a differenza di quanto accaduto con la Direttiva Madre, accoglie la precisazione svolta dal Gruppo di lavoro intesa ad escludere dal novero dei dati rilevanti per la normativa quelli relativi

[104] Il titolo X ("Comunicazioni elettroniche") rappresenta la sezione del Codice emanata in attuazione, non della disciplina generale, ma della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, la quale, come visto nel capitolo primo, contempla espressamente la facoltà di estendere la disciplina anche alle persone giuridiche. Segnatamente, secondo l'interpretazione del Garante, la sostituzione del termine "abbonato" con quella di "contraente", avvenuta ad opera del D.lgs. 28 maggio 2012, n. 69, attuativo della Direttiva 2009/136/CE recante modifiche, fra l'altro, della direttiva 2002/58/CE, quale destinatario del capo I del titolo X del Codice, conferma la volontà del legislatore di tutelare anche le persone giuridiche nel contesto delle comunicazioni elettroniche.

[105] Garante per la protezione dei dati personali, Provvedimento in ordine all'applicabilità alle persone giuridiche del Codice in materia di protezione dei dati personali a seguito delle modifiche apportate dal d.l. n. 201/2011 (Pubblicato sulla Gazzetta Ufficiale n. 268 del 16 novembre 2012; Registro dei provvedimenti n. 262 del 20 settembre 2012).

ai defunti.[106] Tuttavia, anche in tale ipotesi, si impongono chiarimenti simili a quelli illustrati per i dati relativi alle persone giuridiche.

In primo luogo, è sempre possibile che informazioni attinenti ad un soggetto deceduto possano riguardare anche chi è ancora in vita. Secondo il Gruppo, sussistono casi in cui i dati continuano comunque a godere di una protezione indiretta, segnatamente "quando le informazioni costituenti dati di un defunto possono considerarsi concernenti nel contempo anche persone viventi e configurare dati personali soggetti alla direttiva".[107] L'esempio più evidente è quello dei dati genetici che, potendo interessare i membri della medesima famiglia, consentono di ricavare informazioni, anche sensibili, relative ai consanguinei del defunto.[108] Alcune problematiche potrebbero sorgere, invece, per i dati che non sono direttamente collegati alle persone fisiche viventi, ma che potrebbero comunque permettere un'identificazione tramite la combinazione con altre informazioni. In tal senso, un esempio potrebbe riguardare le informazioni relative alla residenza del defunto: può qualificarsi come dato non personale e, pertanto, sottrarsi dalle prescrizioni del GDPR? La risposta a tale quesito dipende, come spesso si è sostenuto nell'ambito del presente lavoro, dalle circostanze del caso concreto. Il dato dovrà essere trattato come personale se, nella fattispecie, il defunto condivideva la residenza con il coniuge o altro familiare, atteso che con l'ausilio di informazioni aggiuntive – il rapporto di

[106] Regolamento (UE) 2016/679, cons. n. 27.
[107] Gruppo di lavoro articolo 29, "*Parere 4/2007 sul concetto di dati personali*", *op. cit*., pp. 22-23.
[108] Per un approfondimento, anche dei profili definitori, in materia di dati genetici, si rimanda a: IANNUZZI A., FILOSA F., *Il trattamento dei dati genetici e biometrici*, in *Dirittifondamentali.it*, Fascicolo 2/2019.

coniugio o parentela – risulta estremamente semplice risalire alla residenza del soggetto ancora in vita.

In secondo luogo, il considerando n. 27 del GDPR lascia ampia discrezionalità ai legislatori nazionali, i quali "possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute". Di nuovo, si rivela interessante analizzare il panorama italiano, nel contesto del quale il decreto legislativo 101 del 2018, avvalendosi della facoltà garantita dalla normativa europea, ha inserito nel Codice privacy l'articolo 2-terdecies, rubricato "Diritti riguardanti le persone decedute". Come ha precisato il Garante per la protezione dei dati personali italiano in un recente parere,[109] il ricorso alla "clausola di salvaguardia" effettuato dal nostro ordinamento si è tradotto nel riconoscimento dei diritti previsti dagli articoli dal 15 al 22 del GDPR a "chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione".[110] Invero, il Garante legge in questa disposizione una *fictio iuris* volta ad equiparare i dati dei deceduti a quelli dei viventi. In tesi, il riconoscimento dei diritti tipici del *data subject* presuppone l'integrale applicazione della disciplina in materia di protezione dei dati personali.[111]

A ben vedere, l'interpretazione proposta espone il fianco ad alcune critiche di carattere pragmatico, incentrate sulla sussistenza di una effettiva equiparazione tra dati relativi ai viventi e dati relativi ai defunti. La volontà del legislatore di individuare in maniera specifica le disposizioni da rendere applicabili anche alle informazioni relative ai deceduti sembra contraddire una completa

[109] Garante per la protezione dei dati personali, Parere su una istanza di accesso civico - 10 gennaio 2019 (doc. web n. 9084520).
[110] Decreto legislativo 30 giugno 2003, n. 196, art. 2-*terdecies*, comma 1.
[111] Garante per la protezione dei dati personali, Parere su una istanza di accesso civico, *cit.*

equivalenza delle due figure e, di conseguenza, una piena applicazione di tutto l'impianto regolamentare in materia di dati personali. Pertanto, i puntuali riferimenti agli articoli da 15 a 22 tagliano fuori gli altri istituti del GDPR, quali, a titolo di esempio, la valutazione d'impatto o il trasferimento verso Paesi terzi. Tali interrogativi avrebbero meritato maggiore approfondimento da parte delle istituzioni europee, atteso che la discrezionalità legislativa riconosciuta dal regolamento cela alcune insidie derivanti dalla potenziale eterogeneità delle discipline fra Stati membri, in un settore, quello dei dati dei deceduti, in forte crescita. Nell'era della datificazione, dove sempre più "persone elettroniche" sopravvivono alle persone reali dalle quali originano, il carattere transnazionale dei dati, anche di quelli relativi ai deceduti, rischia di entrare in crisi di fronte a meccanismi di tutela post-mortale estremamente diversi.[112]

d) Identificata o identificabile

L'ultimo elemento analizzato dal Gruppo di lavoro racchiude due componenti distinte, che si pongono in successione logica l'una con l'altra. Se una persona fisica è "identificata" quando viene distinta da tutti i membri appartenenti al medesimo gruppo, essa risulta "identificabile" quando l'operazione di identificazione non è ancora avvenuta, ma sussiste la possibilità di portarla a termine con successo.[113] L'identificabilità costituisce la zona di confine della categoria del dato a carattere personale, superata la quale si rientra nel novero dei dati non personali. La complessità insita nell'individuazione del vero significato di tale nozione si percepisce anche dalla disposizione del GDPR dedicata alla definizione del dato

[112] Per un approfondimento in materia, si veda: RESTA G., *La "morte" digitale*, in *Il diritto dell'informazione e dell'informatica*, Anno XXIX, Fasc. 6-2014, pp. 891 e ss.
[113] Gruppo di lavoro articolo 29, "*Parere 4/2007 sul concetto di dati personali*", *op. cit*., p. 12.

personale. Il termine identificabile è l'unico tra i quattro analizzati per il quale il legislatore ha ritenuto necessaria un'ulteriore specificazione, affermando che "si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".[114]

Innanzitutto, il Gruppo svolge un interessante rilievo nel delineare puntualmente l'operazione di identificazione secondo il significato che assume nel contesto della disciplina europea. Essa, infatti, non deve avvenire necessariamente attraverso il nome dell'interessato, il quale rimane solamente il metodo più comune, ma non l'unico, per distinguere una persona fisica dalle altre. Oggi, ancor più che nel periodo in cui il parere del Gruppo fu licenziato, pressoché ogni individuo è associabile in maniera univoca ad un dispositivo mobile che lo segue in ogni spostamento e che contiene una quantità sterminata di dati che permettono di definirne la personalità e il comportamento.[115] Sulla scorta di tale osservazione, il Gruppo afferma, a ragione, che per considerare un individuo identificato è sufficiente avere a disposizione quei riferimenti che offrono la possibilità di categorizzarlo e separarlo dagli altri membri della collettività, anche nei casi in cui non si pervenga ad una effettiva conoscenza del suo nominativo.[116]

---

[114] Art. 4, punto 1), Regolamento (UE) 2016/679.
[115] ZUIDERVEEN BORGESIUS F., *Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation*, in *Computer Law & Security Review*, 2016, pp. 256 e ss.
[116] Gruppo di lavoro articolo 29, "*Parere 4/2007 sul concetto di dati personali*", *op. cit*., pp. 14-15.

In secondo luogo, il parere precisa che tanto per l'identificazione diretta quanto per quella indiretta giocano un ruolo chiave i cosiddetti "identificatori", ossia le informazioni collegate ad una determinata persona fisica che, in quanto tali, ne consentono l'identificazione. In questo senso, se gli identificatori diretti permettono di addivenire ad una identificazione completa anche senza l'utilizzo di informazioni aggiuntive,[117] ciò non avviene per quelli indiretti che richiedono il ricorso a quello che il Gruppo di lavoro chiama "fenomeno delle combinazioni uniche".[118] Gli identificatori indiretti, consistendo in una serie di attributi che non mostrano un immediato collegamento con una determinata persona fisica,[119] non rendono possibile l'identificazione univoca in via autonoma, ma solamente attraverso combinazioni reciproche o con altre informazioni aggiuntive provenienti da fonti esterne.[120]

Simili variabili concorrono ad ampliare il margine interpretativo di un concetto cardinale per la definizione della classe dei dati personali come quello di identificabilità. Pertanto, ai fini di una migliore comprensione della nozione in esame, è opportuno tornare sul considerando n. 26 del GDPR – e della Direttiva 95/46/CE prima – il quale individua come fattore chiave nella determinazione della sussistenza dell'identificabilità la ragionevole probabilità di utilizzo da parte del titolare o di un terzo dei mezzi necessari all'identificazione.[121]

---

[117] Ad esempio, tra gli identificatori diretti figurano il nome o l'immagine dell'interessato.
[118] Gruppo di lavoro articolo 29, "*Parere 4/2007 sul concetto di dati personali*", *op. cit*., pp. 13-14.
[119] Esempi di identificatori indiretti sono il numero di telefono o l'indirizzo e-mail dell'interessato.
[120] RUNSHAN H. ET AL. *Bridging Policy, Regulation, and Practice?*, *op. cit*.
[121] La parte che qui rileva del considerando n. 26 del GDPR recita: "Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione

In tal caso, il Gruppo di lavoro tradisce una ambiguità di fondo, frutto delle già importanti incertezze che avvolgono la definizione dei dati. Da un lato, l'esclusione della "sola possibilità ipotetica di distinguere una persona" con cui esordisce la sezione in esame, si ricollega all'atteggiamento possibilista in merito ad una qualificazione "scissa" della natura dei dati, in ragione della quale un'informazione personale per un determinato titolare potrebbe, al ricorrere di circostanze ben precise, considerarsi non personale per un soggetto terzo.[122] Il passaggio – che verrà poi implicitamente smentito nella successiva opinione del Gruppo relativa all'anonimizzazione – risulta particolarmente rilevante in quanto sembra fornire una chiave di interpretazione restrittiva dell'insieme dei mezzi che possono essere ragionevolmente utilizzati anche "da altri" per identificare.[123] Dall'altro lato, invece, il Gruppo opta per una caratterizzazione estremamente ampia dell'elemento dell'identificabilità. Oltre al "costo dell'identificazione", alla "finalità", al "modo in cui viene strutturato il trattamento", al "vantaggio atteso" dal titolare, agli "interessi dei singoli" e al "rischio di disfunzioni organizzative e tecniche", ciò che più colpisce è la necessità di prendere in considerazione le possibilità di avanzamento della tecnologia nel periodo di conservazione dei dati.[124] In tale prospettiva, la logica secondo cui la personalità del dato dipende anche dal periodo di conservazione, unita alla sempre più veloce capacità di sviluppo delle tecnologie ICT, non può che

---

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".

[122] Gruppo di lavoro articolo 29, "*Parere 4/2007 sul concetto di dati personali*", *op. cit*., pp. 17-21.

[123] ZUIDERVEEN BORGESIUS F., *Singling out people without knowing their names, op. cit*.

[124] Gruppo di lavoro articolo 29, "*Parere 4/2007 sul concetto di dati personali*", *op. cit*., p. 15.

portare ad una concezione della soglia di identificabilità piuttosto bassa. [125]

Il contenuto concreto dell'elemento dell'identificabilità è stato delineato anche dalla Corte di giustizia nella citata sentenza *Breyer*. Fondandosi sul presupposto che i mezzi per realizzare l'identificazione possono essere nella disponibilità di soggetti diversi, la Corte esamina la ragionevolezza dell'utilizzo degli strumenti necessari a realizzare l'identificazione.[126] Mentre nel caso di specie i giudici hanno individuato immediatamente un canale di comunicazione tra il titolare che trattava informazioni identificabili e quello che possedeva le informazioni aggiuntive, non è ancora chiaro se, in circostanze in cui il collegamento fra i soggetti coinvolti non è così evidente, sia corretto giungere alla medesima conclusione.[127]

La dilatazione del significato del considerando n. 26 proposta dalla Corte di giustizia nella sentenza in parola sembra, tuttavia, incontrare alcuni limiti che contribuiscono a rendere l'elemento della ragionevolezza maggiormente aderente ad una visione moderna e consapevole del mondo dei dati. Nel confronto tra il criterio ermeneutico "oggettivo", secondo cui il dato è qualificabile come personale per tutti i titolari coinvolti, anche se la reale possibilità di

---

[125] DALLA CORTE L., *Scoping Personal Data, op. cit*. Tra l'altro, in quest'ottica, è ravvisabile una correlazione e una continuità logico-giuridica fra la nozione di dato personale e la recente Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, 21 aprile 2021 (COM/2021/206 final). Per un approfondimento in merito alla relazione che lega tale Proposta, che si propone di non pregiudicare l'applicabilità del GDPR e la protezione dei dati personali, si veda: CONTALDI G., *Intelligenza artificiale e dati personali,* in *Ordine internazionale e diritti umani*, n. 5/2021, pp. 1193-1213.

[126] Corte di Giustizia, causa C-582/14, Breyer, *cit*., parr. 42-49.

[127] URGESSA W., *The Protective Capacity of the Criterion of "Identifiability" Under EU Data Protection Law*, in *European Data Protection Law Review* (EDPL), vol. 2, no. 4, 2016, p. 524; MOURBY M. ET AL., *Are 'pseudonymised' data always personal data?*, *op. cit*., p. 226.

identificare l'interessato compete solamente ad alcuni di essi, e il criterio "relativo", che ammette una duplice natura del dato a seconda del contesto in cui opera il titolare interessato,[128] i giudici non danno segno di un approccio fideistico al primo dei due criteri. Ne deriva una visione dell'elemento dell'identificabilità più moderata rispetto a quella proposta dal Gruppo di lavoro.[129] Nel ravvisare l'irragionevolezza dell'utilizzo dei mezzi di identificazione – e la conseguente fuoriuscita dei dati dal novero di quelli personali – oltre che nelle situazioni di impossibilità oggettiva, anche nelle ipotesi in cui l'identificazione viene vietata dalla legge,[130] la Corte si sta dimostrando favorevole ad una visione contestuale della natura del dato, che non si focalizza solamente sull'informazione in sé considerata, ma che prende come parametro di riferimento l'ambiente in cui opera il titolare del trattamento, incluse le eventuali strade che lo potrebbero collegare ad un soggetto terzo che dispone delle informazioni aggiuntive utili a conseguire con successo l'identificazione.[131]

Tornando al testo del GDPR, la prima critica che la dottrina muove nei confronti della disciplina europea concerne l'equiparazione fra i dati che si riferiscono alla persona identificata e quelli che riguardano la persona identificabile, poiché non sembra conferire il giusto peso al superiore grado di de-identificazione presente nel secondo caso.[132] Tale scelta legislativa viene reputata dai detrattori come antagonista delle politiche di de-identificazione:

---

[128] Corte di Giustizia, causa C-582/14, Breyer *c*. Bundesrepublik Deutschland, *cit*., par. 25.
[129] PURTOVA N., *The Law of Everything*, *op. cit*., pp. 62-65.
[130] Corte di Giustizia, causa C-582/14, Breyer, *cit*., par. 46.
[131] IRTI C., *Personal Data, Non-Personal Data, Anonymised Data, Pseudonymised Data, De-identified Data*, in SENIGAGLIA R., IRTI C., BERNES A. (eds.), *Privacy and Data Protection in Software Service*, Springer, 2022, pp. 49-51.
[132] SCHWARTZ P., SOLOVE D., *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, in *New York University Law Review*, Vol. 86, 2011, pp. 1873-1877.

se gli obblighi sono gli stessi tanto per i dati relativi alle persone identificate, quanto per quelli relativi alle persone identificabili, il titolare non avrà alcun incentivo ad applicare misure di sicurezza per mezzo di de-identificazione.[133]

Invero, in risposta a tale orientamento, è doveroso precisare che i dati sottoposti ad un procedimento di de-identificazione, come nel caso di quelli pseudonimizzati illustrati in precedenza, permettono di beneficiare di un regime normativo più favorevole rispetto a quello che riguarda i dati personali comuni.[134] La stessa corretta implementazione dei principi di *privacy by design* e di *privacy by default*, sebbene carenti del carattere prescrittivo tipico delle norme di dettaglio, traducono comunque la volontà del legislatore di ridurre al minimo i rischi derivanti dal trattamento dei dati personali, anche attraverso misure tecniche ed organizzative volte a ridurre l'identificabilità degli interessati. Pertanto, lo stimolo ad implementare misure di de-identificazione è comunque presente, se non grazie a una cultura digitale non ancora sufficientemente diffusa, almeno per merito di disposizioni normative che privilegiano chi segue tale via.[135]

Peraltro, alcuni autori segnalano la ormai sopravvenuta carenza di rilevanza della distinzione tra persona identificata ed identificabile alla luce della aumentata capacità di analisi degli strumenti moderni e della possibilità di ricorrere ad una quantità crescente di informazioni liberamente accessibili.[136] Se ormai la realtà digitale è costituita principalmente dai cosiddetti "*high*-

[133] HINTZE M., *Viewing the GDPR through a de-identification lens*, *op. cit.*
[134] *Supra*, par. 2.1.
[135] FINCK M., PALLAS F., *They who must not be identified*, *op. cit.*, pp. 35-36.
[136] TENE O., POLONETSKY J., *Big Data for All: Privacy and User Control in the Age of Analytics*, in *Northwestern Journal of Technology and Intellectual Property*, Vol. 11, Issue 5, 2013, pp. 257-259.

dimensional data", ossia da un numero di attributi relativi ad un individuo così elevato da consentire agevolmente di collegare un dato alla relativa persona fisica in maniera univoca,[137] trasformare un interessato "identificabile" in "identificato" è diventata un'operazione più semplice rispetto al passato.

Altro fattore su cui si soffermano le critiche della dottrina riguarda l'effetto espansivo che l'identificabilità produce nei confronti della categoria del dato personale. Di fronte all'alternativa secca predisposta dal legislatore europeo, l'elemento dell'identificabilità ha costantemente favorito un notevole allargamento dell'area del dato personale, conducendo verso l'applicazione delle garanzie accordate all'individuo anche in situazioni in cui il rischio di lesione del diritto fondamentale risulta minimo, se non addirittura nullo.[138] L'approccio manifestato dal Gruppo di lavoro si avvicina sin troppo ad un'impostazione oggettiva, ben lontana da quel criterio di ragionevolezza che dovrebbe guidare l'interprete nella ricerca della natura del dato.[139] Il punto di caduta di una prospettiva simile si rinviene in un ambito di applicazione del GDPR eccessivamente dilatato, potenzialmente capace di coprire ogni informazione in circolazione, che dà vita ad una disciplina sulla protezione dei dati personali incerta e di dubbia efficacia.[140]

Pertanto, anche a seguito dell'esame del concetto di identificabilità, risulta palese che le criticità che affliggono la

---

[137] NARAYANAN A., FELTEN E.W, *No silver bullet: De-identification still doesn't work*, 2014.
[138] FOGLIA C., *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione nel GDPR*, in PANETTA R. (a cura di), *Circolazione e protezione dei dati personali tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, 2019, pp. 309-332.
[139] ZWENNE G., *Diluted Privacy Law*, Universiteit Leiden, 2013.
[140] PURTOVA N., *The Law of Everything, op. cit*. pp. 75-78.

categoria del dato personale impongono una rivisitazione dell'approccio statico adottato dalle istituzioni europee. Le svariate soluzioni prospettate in sede dottrinale, che oscillano da una semplice rilettura delle disposizioni vigenti sino alla prospettazione di una vera e propria riforma del *data law*, possono essere comprese e valutate solamente dopo aver analizzato anche l'altro versante della materia, quello dei dati non personali.

3. Il dato non personale

Una disamina onnicomprensiva del mondo dei dati non può prescindere dunque dall'esame della fattispecie del dato non personale. Sebbene il legislatore europeo abbia costruito l'impianto regolamentare sulla base di una separazione apparentemente nitida tra dati personali e non personali, le due categorie sono legate, piuttosto, da uno rapporto di continuità,[141] specie a causa del carattere residuale dei secondi rispetto ai primi. Alla crescita esponenziale della quantità di dati non personali nel periodo recente, per merito principalmente della diffusione di fenomeni quali l'*Internet of Things*, la *smart manufacturing*, la *data analysis* e il *digital marketing*, si è accompagnata una maggiore attenzione al tema, tanto sul versante legislativo quanto su quello dottrinale.

In ambito europeo, è il Regolamento (UE) 2018/1807 a positivizzare per la prima volta una definizione normativa dei dati a carattere non personale. Malgrado le lacune lasciate dal Regolamento in parola – in parte illustrate nel corso del capitolo precedente – nei paragrafi seguenti ci si focalizzerà essenzialmente sui profili definitori della fattispecie e sulle sue articolazioni.

[141] SCHWARTZ P., SOLOVE D., *The PII Problem*, *op. cit.*, p. 1876.

L'articolo 3, punto 1, del Regolamento 1807 definisce i dati non personali come "i dati diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679", dunque qualsiasi informazione non riguardante una persona fisica identificata o identificabile. È evidente sin dal principio che se la capacità di distinguere tra dato personale e non personale risulta essenziale in fase di applicazione delle normative alle rispettive categorie di dato, l'adozione di una definizione "negativa" rischia di ripercuotersi sull'efficacia dei due regolamenti.[142] Nei fatti, la residualità che si accompagna ad una terminologia simile potrebbe dipingere la nozione di dato non personale come una via di uscita per i gestori dei dati dalle stringenti prescrizioni in materia di tutela dei dati personali,[143] atteso che tale qualifica comporta la fuoriuscita dall'insieme di regole che il GDPR prescrive con riguardo, oltre che ai diritti degli interessati, agli altri istituti relativi, fra l'altro, all'implementazione delle misure sicurezza, al controllo delle autorità amministrative indipendenti e al trasferimento dei dati al di fuori dell'Unione.[144]

Nel tentativo di dare corpo ad una disposizione che, forse per eccessivo ossequio alla residualità del Regolamento 1807 rispetto al GDPR, si dimostra abbastanza laconica, è stato demandato alla

[142] Parere del CESE sulla Proposta di regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, *op. cit*. In particolare: "il CESE sottolinea la necessità che il regolamento definisca esplicitamente i dati non personali e che non vi sia soltanto una definizione generica o complementare a quella di cui al regolamento (UE) 2016/679, dal momento che molte giurisdizioni hanno interpretato in maniera diversa le nozioni di dati personali e non personali". A tal proposito, si veda: MONTAGNANI M. L., *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in *Mercato Concorrenza Regole, Rivista quadrimestrale*, 2/2019, pp. 304-310.

[143] GRAEF I., GELLERT R., HUSOVEC M., *Towards a holistic regulatory approach for the European data economy: Why the illusive notion of non-personal data is counterproductive to data innovation*, in *TILEC Discussion Paper No. 2018-029*, 2018, pp. 1-3.

[144] Corte di Giustizia, causa C-434/16, Nowak, *cit*., par. 49.

Commissione europea il compito di pubblicare orientamenti informativi utili all'interpretazione delle nuove disposizioni. [145] Conseguentemente, la *Guidance* pubblicata nel maggio 2019 si è rivelata più che opportuna, in quanto contenente una specificazione della nozione di dato non personale con una dovizia di dettagli maggiore rispetto a quanto fatto dal testo legislativo.[146]

A tale proposito, malgrado la classificazione fornita dalla Commissione non possa vantare un valore prescrittivo pari a quello delle disposizioni del Regolamento 1807,[147] il documento fotografa in maniera adeguata lo stato dell'arte della circolazione dei dati non personali nel territorio europeo e, pertanto, costituisce un utile punto di partenza per lo studio della fattispecie. Adottando come angolo visuale la fonte da cui origina l'informazione, la Commissione esordisce distinguendo all'interno della categoria "dato non personale" due sottoinsiemi differenti.[148] Da un lato, si trovano le informazioni che "in origine non si riferivano a una persona fisica identificata o identificabile", fra le quali figurano, a titolo di esempio, i dati sulle condizioni meteorologiche prodotti da sensori o i dati sulle esigenze di manutenzione delle macchine industriali. Ai fini del presente lavoro, tali informazioni verranno definite come

[145] Art. 8, par. 3, Regolamento (UE) 2018/1807.
[146] Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union* (COM (2019) 250 final).
[147] Lo stesso documento sottolinea sin da subito il carattere puramente informativo della guida della Commissione: "Il presente documento è fornito dalla Commissione europea esclusivamente a titolo informativo. Esso non contiene alcuna interpretazione autorevole del 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, né costituisce una decisione o un'opinione della Commissione europea. Tale documento non pregiudica eventuali decisioni o opinioni della Commissione europea, né le competenze della Corte di giustizia dell'Unione europea per l'interpretazione del regolamento conformemente ai trattati dell'UE".
[148] Comunicazione della Commissione, *Guidance*, *op. cit.*, p. 6.

industriali o a-personali.[149] Dall'altro lato, invece, si trovano quei dati che sono nati come personali, ma che sono stati anonimizzati in un secondo momento. In tal caso, il sintagma utilizzato nel presente lavoro sarà quello di "dati anonimizzati", da distinguere da quello di "dati anonimi", spesso impiegato dalla dottrina per indicare l'intero insieme dei dati a carattere non personale. Tale tipologia di informazioni pone maggiori problemi con riguardo alla esatta individuazione della loro natura. Nonostante l'anonimizzazione si presenti come il metodo di de-identificazione più robusto fra quelli disponibili, vari esperimenti hanno dimostrato che, se eseguita in maniera impropria, il procedimento può essere invertito e gli interessati re-identificati.[150]

In sostanza, anche la qualifica di dato anonimizzato si trova in rapporto di stretta dipendenza con l'interpretazione dell'elemento dell'identificabilità. Lo stesso considerando n. 26 del GDPR inferisce dall'accertamento dell'assenza di ragionevole probabilità di utilizzo dei mezzi necessari per identificare l'interessato, l'estromissione delle informazioni anonime, comprese quelle anonimizzate, dall'ambito di applicazione della disciplina.[151]

Nei paragrafi che seguono si tenterà di evidenziare come la necessità di riformare la visione europea in materia di *data law*, già vista con riferimento al dato personale, risulti palese anche con riguardo alle sottocategorie del dato a carattere non personale.

---

[149] ELLIOT M., MACKEY E., O'HARA K., TUDOR C., *The anonymisation decision-making framework*, *Ukan Publications*, 2016, p. 9.

[150] URGESSA W., *The Protective Capacity of the Criterion of "Identifiability" Under EU Data Protection Law*, *op. cit*. pp. 528-529.

[151] Il quinto periodo del considerando n. 26 recita: "I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato".

3.1 Il dato anonimizzato

3.1.1 Anonimizzazione e rischio di re-identificazione

Un dato anonimizzato è considerato non personale solamente se i mezzi impiegati per il trattamento non permettono di ricondurre l'informazione in esso contenuta ad una persona fisica identificata o identificabile. Lo scopo delle tecniche di anonimizzazione è, quindi, quello di eliminare il collegamento sussistente tra l'informazione semantica contenuta nel dato e la persona fisica cui esso fa riferimento. Tale risultato non viene ottenuto per mezzo della semplice cancellazione degli identificatori diretti, ma, in una prospettiva più ampia, il trattamento in esame mira ad impedire che la re-identificazione possa avvenire anche ricorrendo ad analisi incrociate con altri *dataset* disponibili.[152] Non si tratta di una misura di sicurezza più robusta della pseudonimizzazione, ma di un processo capace di alterare la natura delle informazioni.[153] I dati anonimizzati, infatti, si distinguono da quelli pseudonimizzati in virtù dell'impossibilità di attribuirli ad una persona specifica anche ricorrendo ad informazioni aggiuntive.[154]

Sfortunatamente, tale rappresentazione teorica non corrisponde alla realtà dei fatti. In uno degli articoli dottrinali più influenti della storia recente, Paul Ohm ha evidenziato come il progresso tecnologico e la crescita della disponibilità di *dataset* abbiano infranto l'illusione, alla base della maggior parte delle discipline in materia di protezione dei dati, secondo cui

[152] GRUSCHKA N., MAVROEIDIS V., VISHI K., JENSEN M., *Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR, 2018 IEEE International Conference on Big Data (Big Data)*, 2018.
[153] In ogni caso, dal momento in cui interviene su dati, inizialmente a carattere personale, anche il procedimento di anonimizzazione rientra nella definizione di "trattamento" di cui all'art. 4, punto 2) del GDPR.
[154] Comunicazione della Commissione, *Guidance*, *op. cit.*, p. 6.

l'anonimizzazione tradizionalmente intesa è capace di garantire una definitiva de-identificazione.[155] Nella prospettiva dell'autore, una procedura in grado di generare dati anonimi al punto da rendere impossibile per un eventuale *intruder*, ossia il soggetto che mira alla re-identificazione, il raggiungimento del proprio scopo può essere ottenuta solamente sacrificando qualsiasi utilità del dato.[156] Da tali considerazioni nasce il dibattito accademico tra chi continua a valutare le tecniche di anonimizzazione come uno strumento ancora efficace per localizzare il punto di equilibrio tra protezione dei dati e libera circolazione,[157] e chi, al contrario, dimostra particolare cautela, se non sfiducia, nelle capacità salvifiche di tale modello.[158]

Al fine di comprendere come le istituzioni europee abbiano approcciato un tema così delicato per la protezione dei dati si rivela di nuovo utile fare riferimento a quello che, ancora oggi, risulta essere uno dei documenti di riferimento nel campo dell'anonimizzazione: l'opinione 05/2014 adottata dal Gruppo di lavoro articolo 29 nel 2014.[159] Al suo interno, l'anonimizzazione viene in un primo momento descritta come un trattamento effettuato sui dati personali volto a prevenire l'identificazione del soggetto in maniera irreversibile, ossia senza che il processo possa essere compiuto a ritroso. Tuttavia, nel prosieguo dell'analisi, il Gruppo di lavoro sembra alternare a questa iniziale definizione piuttosto

[155] OHM P., *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, UCLA Law Review, Vol. 57, 2010, pp. 1701 e ss.
[156] *Ibid*. Con parole perentorie, l'A. afferma: "Data can be either useful or perfectly anonymous but never both", p. 1704.
[157] CAVOUKIAN A., CASTRO D., *Big Data and Innovation, Setting the Record Straight: De- identification Does Work*, 2014.
[158] NARAYANAN A., SHMATIKOV V., *Myths and Fallacies of Personally Identifiable Information*, in *Communications of the ACM*, vol. 53, no. 6, 2010, pp. 24 e ss.; NARAYANAN A., FELTEN E.W, *No silver bullet: De-identification still doesn't work, op. cit*.
[159] Article 29 Data Protection Working Party (WP29), "*Opinion 05/2014 on Anonymisation Techniques*" (WP216).

rigorosa, un diverso approccio che più volte richiama il fattore del rischio residuo di re-identificazione che si cela dietro ad ogni processo di anonimizzazione.[160] Infatti, viene specificato che, dopo l'avvenuto trasferimento del dataset anonimizzato dal titolare originario ad una terza parte, la disciplina relativa alla protezione dei dati personali continuerà, o comunque tornerà, ad avere applicazione se il ricevente opera in un contesto, con mezzi di trattamento e perseguendo finalità che comportano un inaccettabile rischio di re-identificazione.[161]

Questo secondo approccio appare ben più consapevole ed ancorato ad una realtà in cui il potenziamento delle tecnologie di analisi dei dati unito al proliferare delle politiche a sostegno dell'*open access*,[162] hanno reso l'anonimizzazione rigorosamente intesa un'utopia. Presupponendo che non è mai possibile azzerare la probabilità che il soggetto cui il dato anonimo inerisce sia identificato, l'irreversibilità è ormai qualche cosa che non può più essere pretesa in senso assoluto,[163] ma è un obiettivo cui il titolare del trattamento deve aspirare al fine di portare il rischio di re-identificazione al di sotto di una soglia ritenuta accettabile.

In tale ipotesi, la dirompente forza centripeta che accompagna lo sviluppo delle tecnologie dei *Big Data* rende necessario un cambiamento di paradigma anche in riferimento all'anonimizzazione, in modo tale da abbandonare la concezione statica che sembra

[160] STALLA-BOURDILLON S., KNIGHT A., *Anonymous data v. Personal Data – A false debate: an EU perspective on anonymization, pseudonymization and personal data*, in *Wisconsin International Law Journal*, 2016, pp. 12-16.
[161] WP29, *Opinion 05/2014, op. cit*., p. 10.
[162] Si ricordano a titolo esemplificativo: la Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico; la Raccomandazione (UE) 2018/790 della Commissione del 25 aprile 2018 sull'accesso all'informazione scientifica e sulla sua conservazione.
[163] STALLA-BOURDILLON S., KNIGHT A., *Anonymous data v. Personal Data, op. cit.*, pp. 12-16.

permeare – quantomeno in parte – la visione europea, per abbracciare un'impostazione dinamica, consapevole della possibilità che un dato anonimizzato possa tornare ad essere personale,[164] e che si declini in normative di settore e codici di condotta capaci di definire standard comuni.[165] Una politica di così vasta portata, "stante l'impossibilità di tracciare un vademecum per l'anonimizzazione valido in ogni situazione", [166] dovrebbe avere come protagonista un legislatore europeo votato alla promozione di misure, anche di *soft law*, volte a favorire la collaborazione di enti privati e pubbliche amministrazioni operanti in settori affini, eventualmente incentivando l'impiego delle cosiddette *trusted third parties*, come ipotizzato dall'Information Commissoner's Office britannico.[167] Lo scopo di questa operazione sarebbe quello di sviluppare un approccio unitario con riferimento all'anonimizzazione dei dati e alla loro successiva *disclosure*, al fine di ridurre il rischio di re-identificazione attraverso una comunicazione costante fra i soggetti interessati.[168]

Dunque, come si evince dalle considerazioni svolte poc'anzi, la questione giuridica centrale attorno a cui ruotano gli interrogativi

[164] *Ibid*., pp. 28-37.
[165] WP29, *Opinion 05/2014, op. cit*., p. 6. Sempre il medesimo documento sottolinea come l'assenza di standard normativi comunitari sia una delle principali lacune del sistema attuale. Sul problema della mancanza di standardizzazione nell'economia dei dati, si veda: MONTAGNANI M. L., *La libera circolazione dei dati al bivio, op. cit.*, pp. 304-310.
[166] FOGLIA C., *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione nel GDPR, op. cit*., p. 311.
[167] INFORMATION COMMISSIONER'S OFFICE (ICO), *Anonymisation: managing data protection risk code of practice*, 2012, pp. 41-43. Una *trusted third party* è un'organizzazione creata in virtù di un accordo fra parti che vogliono anonimizzare i dati a loro disposizione per poterli poi utilizzare in un progetto comune. Il suo compito è quello di procedere all'anonimizzazione dei dati personali trasferiti dai titolari del trattamento partecipanti all'accordo affinché tutte le parti possano beneficiarne. È molto utile nell'ambito della ricerca scientifica, in quanto permette ai centri di ricerca di avere accesso ai dati, senza che si configuri un trattamento di dati personali e, di conseguenza, senza l'ulteriore onere di assumere la qualifica di titolare del trattamento.
[168] *Ibid.*, p. 40. Ad esempio, questo dialogo potrebbe impedire che enti appartenenti allo stesso settore pubblichino dataset anonimizzati i quali, riferendosi alle medesime aree geografiche, aumenterebbero di gran lunga la probabilità che la re-identificazione abbia successo

riguardanti la tematica dell'anonimizzazione concerne principalmente la disciplina del rischio; in particolare, la sua gestione, ossia le modalità attraverso cui effettuare la sua valutazione, da un lato, e il suo grado di accettabilità in concreto, cioè la soglia al di sotto della quale esso può considerarsi tollerabile, dall'altro. La prospettiva antecedente all'avvento della società digitale, caratterizzata dalla possibilità di garantire una irreversibilità permanente, faceva sì che la distinzione tra dato personale e dato anonimo fosse lineare e statica, in quanto il dato non sarebbe mai potuto tornare ad essere collegato ad una persona fisica.[169] Oggi, invece, questa impostazione non è più plausibile poiché la possibilità di portare a termine la re-identificazione con successo non può mai essere esclusa con assoluta certezza. Di conseguenza, si può affermare che il dato anonimizzato abbia subito un mutamento radicale nei suoi caratteri essenziali, trasformandosi in una struttura giuridica in forza della quale viene garantito un certo equilibrio tra un rischio (giuridicamente) improbabile di re-identificazione – e, in quanto tale, qualificato come accettabile dal punto di vista normativo – e il principio di libera circolazione dei dati all'interno dell'Unione europea. Tuttavia, come verrà precisato nel paragrafo successivo, risulterebbe del tutto illogico calcolare tale rischio adottando esclusivamente il dato anonimizzato come punto di osservazione, poiché verrebbero tralasciati numerosi altri fattori che incidono in misura notevole sulle possibilità di re-identificazione.[170]

In definitiva, siffatti rilievi inducono a sostenere che il dato anonimizzato costituisce un concetto di natura "stipulativa", e non oggettiva, in ragione della intrinseca incapacità di eliminare il rischio

[169] OECD, *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, in *OECD Digital Economy Papers*, No. 176, OECD Publishing, Paris, 2011, pp. 26-28.
[170] OHM P., *Broken Promises of Privacy*, *op. cit.*, pp. 1733-1735.

residuo di re-identificazione che caratterizza l'era della datificazione. Di conseguenza, la qualificazione di informazione anonimizzata non dipende più dalla irreversibilità del processo di de-identificazione, ma si ricollega alla soglia di tollerabilità del pericolo, stabilita in via convenzionale, che la persona fisica originaria possa essere nuovamente identificata. Questo primo profilo del rischio – riconducibile alla dimensione della protezione individuale – si riflette inevitabilmente sul secondo, quello legato alla dimensione della circolazione delle informazioni: il rischio di inutilità del dato. Se è vero che ad un elevato grado di de-identificazione corrisponde una significativa diminuzione dell'utilità del dato,[171] la minore "sfruttabilità" delle informazioni che ne deriva non può che disincentivare la libera circolazione.

Pertanto, anche in seno a tale peculiare dimensione del *data law*, si profila il tipico busillis giuridico consistente nel corretto bilanciamento di diritti e interessi contrapposti. Sul legislatore ricade, dunque, l'onere di rintracciare il giusto punto di equilibrio tra esigenze di anonimizzazione, in funzione protettiva delle persone fisiche, ed esigenze di sfruttamento dei dati, ossia di tutela della circolazione come elemento imprescindibile per lo sviluppo della *data driven innovation*.

Peraltro, il continuo mutamento delle regole tecniche nell'ambito dell'analisi dei dati, il quale non consente di fare assegnamento su un bilanciamento statico e definitivo, suggerisce al legislatore di abbandonare la prospettiva focalizzata esclusivamente sul risultato finale, ossia il "dato anonimizzato", per dedicare, invece, maggiore attenzione al processo che lo precede: la de-identificazione nel suo complesso. A tal fine, si rivela necessaria

[171] OHM P., *Broken Promises of Privacy*, *op. cit.*

l'introduzione di un nuovo paradigma logico-giuridico dove anonimizzazione e pseudonimizzazione, non vengono più trattate alla stregua di tecniche, o regimi, distinti – come indica il considerando n. 26 del GDPR – ma come misure in continuità fra loro, giacché la loro combinazione assicura maggiori garanzie di successo per il raggiungimento degli obiettivi di minimizzazione dei rischi di re-identificazione e di mantenimento dell'utilità dei dati.[172]

3.1.2 Il design del trattamento residuo in chiave contestuale

Un altro passaggio fondamentale contenuto nell'opinione del 2014 figura nel riferimento alla cancellazione del dataset originale da parte del titolare del trattamento. Il Gruppo di lavoro articolo 29 asserisce che dopo il trasferimento dell'insieme di dati ad una terza parte, preceduto da una corretta anonimizzazione, tali dati saranno considerati personali fintantoché il titolare originario non abbia cancellato in via definitiva il *dataset* originale.[173] La stessa

[172] Invero, lo stesso Data Governance Act oggetto del quarto capitolo, nella versione approvata dal Parlamento, mostra una prima apertura a tale rinnovata impostazione nella parte del cons. n. 15 in cui recita: "Qualora la fornitura di dati anonimizzati o modificati non rispondesse alle esigenze del riutilizzatore, a condizione che siano stati soddisfatti i requisiti di svolgere una valutazione d'impatto in materia di protezione dei dati e consultare l'autorità di controllo ai sensi degli articoli 35 e 36 del regolamento (UE) 2016/679 e qualora i rischi per i diritti e gli interessi degli interessati risultino minimi, potrebbe essere consentito il riutilizzo in loco o remoto dei dati in un ambiente di trattamento sicuro. Ciò potrebbe costituire una soluzione adeguata per il riutilizzo dei dati pseudonimizzati".

[173] WP29, *Opinion 05/2014, op. cit.*, p. 9. In particolare: "[...] it is critical to understand that when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data. Only if the data controller would aggregate the data to a level where the individual events are no longer identifiable, the resulting dataset can be qualified as anonymous. For example: if an organisation collects data on individual travel movements, the individual travel patterns at event level would still qualify as personal data for any party, as long as the data controller (or any other party) still has access to the original raw data, even if direct identifiers have been removed from the set provided to third parties. But if the data controller would delete the raw data, and only provide aggregate statistics to third parties on a high level, such as 'on Mondays on trajectory X there are 160% more passengers than on Tuesdays', that would qualify as anonymous data".

impostazione è stata fatta propria di recente dalla Commissione europea nella guida relativa al Regolamento (UE) 2018/1807.[174]

La scarsa aderenza alla realtà di tale approccio, che ancora oggi informa l'azione delle istituzioni continentali, costituisce il principale punto debole dell'impianto europeo in materia di dati anonimizzati. Difatti, al fine di limitare il più possibile il rischio di re-identificazione, viene assunto come riferimento il dato in sé: se l'informazione è personale anche per uno solamente dei soggetti coinvolti nella catena di trasferimenti, esso deve essere considerato personale anche per tutti gli altri. Benché questa impostazione possa avere (astratti) vantaggi dal punto di vista della tutela dell'individuo, la previsione di obblighi troppo stringenti in capo alle parti coinvolte, se, da un lato si presta ad essere sistematicamente elusa, dall'altro, potrebbe entrare in conflitto con altri diritti e libertà ampiamente riconosciuti a livello continentale (come la libertà di ricerca o il diritto di informazione), oltre che con il principio di libera circolazione dei dati all'interno dell'Unione europea. In tal senso, costringere i titolari a distruggere il *dataset* anche dopo aver eseguito una corretta anonimizzazione rappresenta un chiaro esempio di errato bilanciamento tra esigenze contrapposte. Nell'attuale contesto di *data dependence*, il mantenimento di una misura simile non può che

[174] Comunicazione della Commissione, *Guidance*, *op. cit.*, p. 7, in cui si fa riferimento alla "Opinion 05/2014" del Gruppo di lavoro articolo 29: "soltanto se il responsabile del trattamento [in tal caso è ravvisabile una svista nella traduzione, giacché il termine "*data controller*" della versione in lingua inglese è erroneamente tradotto in "responsabile del trattamento" mentre, al contrario, corrisponde al "titolare del trattamento" nella lingua italiana, *n.d.s.*] aggrega i dati a un livello in cui i singoli eventi non sono più identificabili si può definire anonimo l'insieme di dati risultante. Ad esempio, se un'organizzazione raccoglie dati sugli spostamenti delle persone, i tipi di spostamenti individuali a livello di evento rientrano ancora tra i dati personali per tutte le parti coinvolte, fintantoché il responsabile del trattamento (o altri) ha ancora accesso ai dati non trattati originali, anche se gli identificatori diretti sono stati espunti dall'insieme dei dati forniti a terzi. Tuttavia, se il responsabile del trattamento cancella i dati non trattati e fornisce a terzi solamente statistiche aggregate ad alto livello, ad esempio "il lunedì sulla rotta X i passeggeri sono più numerosi del 160% rispetto al martedì", i dati possono essere definiti anonimi".

tradursi in una pretesa eccessiva o irrealistica, in quanto la minore utilità dei dati conseguente al processo di de-identificazione, produrrebbe un danno, *in primis*, nei confronti dell'attività commerciale del titolare, che cambia strategie e obiettivi a seconda di quello che i dati dicono o possono dire.[175]

Oltretutto, i dati riguardanti vendite, consumi, manutenzione e servizi rappresentano un patrimonio non solo per le aziende che li detengono, ma anche per altri soggetti, pubblici o privati, che potrebbero orientare le proprie scelte e le proprie politiche in base ai risultati derivanti dalle analisi di quelle informazioni. Pertanto, se il titolare non è incentivato a sfruttare legalmente e, quindi, a diffondere i propri dati anche a seguito di anonimizzazione, ripercussioni negative potrebbero aversi in quei settori che non possono prescindere dall'analisi dei dati o dalla loro conservazione. [176] Basti pensare agli organi amministrativi di qualsiasi livello che con più informazioni a loro disposizione prenderebbero decisioni più oculate,[177] oppure ai centri di ricerca che, trovando la loro ragion d'essere nell'analisi dei dati, vedrebbero le proprie potenzialità di sviluppo fortemente ridimensionate.[178]

Viceversa, se l'obiettivo è quello di favorire la *data driven innovation* e, dunque, la circolazione dei dati, è necessario assumere un differente punto di vista che non si focalizzi solo sul dato in sé e per sé, ma che faccia riferimento al soggetto che tratta quel dato, o

[175] Sulla relazione inversamente proporzionale che esiste tra la privacy garantita tramite l'anonimizzazione e l'utilità dei dati anonimizzati si veda: EUROPEAN UNION AGENGY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*, 2015, pp. 27-29.
[176] STALLA-BOURDILLON S., KNIGHT A., *Anonymous data v. Personal Data, op. cit.*, pp. 12-16.
[177] OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, 2015, pp. 407-412.
[178] *Ibid*., pp. 348-355.

meglio, al contesto nel quale tale soggetto opera. In questo scenario, se il titolare originario ha portato a termine l'anonimizzazione in modo corretto e rilasciato il solo *dataset* sottoposto a trattamento pur senza cancellare quello originale –specie in quei casi in cui quest'ultimo è stato protetto tramite adeguate misure di sicurezza come la pseudonimizzazione – il terzo ricevente potrebbe essere considerato in possesso di un insieme di dati anonimi al ricorrere di determinate condizioni e, dunque, non sarebbe titolare del trattamento in riferimento a questi dati.[179] In una prospettiva in cui assume rilevanza il fattore contestuale, per il titolare originario che ancora gode della disponibilità del dataset autentico, il dato sottoposto alla procedura di anonimizzazione continuerà ad essere un'informazione a carattere personale, giacché può facilmente procedere all'identificazione degli individui interessati. Per il terzo, il dato potrà essere non personale se il contesto in cui egli tratta tali informazioni comporta un rischio di re-identificazione inferiore rispetto alla soglia di accettabilità.[180]

Tuttavia, affinché anche l'individuo sia tutelato, è necessario che il titolare proceda preliminarmente ad una attenta valutazione degli strumenti necessari ad invertire il procedimento – in particolare, costi, *know-how* e incremento della disponibilità di dataset *open access* –,[181] anche attraverso verifiche volte a testare l'efficacia della tecnica prescelta, similmente a quanto avviene nei procedimenti di verifica dei sistemi di sicurezza cibernetici.[182] Ulteriori misure tecniche ed organizzative avranno, invece, il duplice

[179] MOURBY M. ET AL., *Are 'pseudonymised' data always personal data?*, *op. cit*.
[180] ELLIOT M. ET AL., *The anonymisation decision-making framework, op. cit*.; ICO, *Anonymisation, op. cit.*, p. 13; STALLA-BOURDILLON S., KNIGHT A., *Anonymous data v. Personal Data, op. cit.*, pp. 12-16.
[181] ELLIOT M. ET AL., *The anonymisation decision-making framework, op. cit*., pp. 55-56.
[182] Irish Data Protection Commission, *Guidance on Anonymisation and Pseudonymisation*, 2019, p. 14.

obiettivo di rendere l'insieme originale sicuro e non reperibile né al terzo ricevente, né ad altre parti che potrebbero poi avere rapporti con tale terzo, e altresì di creare un ambiente digitale in cui i riceventi siano in grado di muoversi solamente all'interno dei margini operativi predisposti dal titolare originario.[183] In aggiunta, un importante ausilio potrebbe derivare da accordi contrattuali che definiscano a chiare lettere quali sono i doveri di entrambe le parti, specificando, tra l'altro, i soggetti legittimati a trattare le informazioni, il tipo operazioni che il terzo può effettuare, gli obblighi che scattano nel caso di re-identificazione fortuita e le responsabilità nel caso di mancato adempimento.[184]

Oltretutto, il titolare dovrebbe porre attenzione al soggetto specifico cui sta per trasferire i dati,[185] poiché le sue caratteristiche influenzeranno considerevolmente il tipo di *disclosure*.[186] Mentre autorizzare l'accesso ai dati anonimizzati ad un gruppo circoscritto di interessati (come potrebbe essere una comunità di ricercatori) permette di gestire in maniera più sicura il rischio di re-identificazione, anche alla luce delle misure regolamentari o contrattuali tese ad innalzare il livello di sicurezza, lo stesso non può dirsi nel caso di pubblicazione generale (ad esempio, su una pagina web liberamente consultabile).[187] In questa seconda ipotesi, il tipo di

---

[183] STALLA-BOURDILLON S., KNIGHT A., *Anonymous data v. Personal Data, op. cit*., pp. 12-16; Gruppo di lavoro articolo 29, "*Parere 4/2007 sul concetto di dati personali*", *op. cit.*, pp. 15-20.

[184] D'ACQUISTO G., NALDI M., *Big data e privacy by design, op. cit.*, p. 37; FOGLIA, *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione nel GDPR, op. cit.*, p. 326.

[185] D'ACQUISTO G., NALDI M., *Big data e privacy by design, op. cit.*, p. 36.

[186] ICO, *Anonymisation, op. cit.*, p. 17. In particolare: "The reason for releasing data will affect how you make the disclosure, because the risk and consequences of identification will differ: • Publication under freedom of information or the open government licence is to the wider world, and carries more risk. • Discretionary disclosures, such as those made for research purposes or in your own commercial interests, can be easier to control and assess but are not without risks".

[187] OHM P., *Broken Promises of Privacy, op. cit.*, pp. 1729-1730.

anonimizzazione da implementare dovrà avere un livello di aggregazione ben più elevato, in virtù del fatto che, una volta che i dati sono entrati nell'oceano digitale, sarà estremamente difficile continuare a tenere sotto controllo il rischio di re-identificazione.[188]

Di fatto, non si sta facendo altro che richiamare ancora una volta l'attenzione su uno dei cardini del GDPR: la *privacy by design*, corredata dai suoi sette principi fondamentali che spingono il titolare a tenere conto dei rischi insiti nel proprio trattamento di dati, fin dalla progettazione dello stesso.[189] Questo principio si traduce, sul piano concreto, nella predisposizione di un *design* del trattamento residuo dei dati in virtù del quale ogni futura operazione effettuata sul dataset originale dovrà, per impostazione predefinita, tenere conto dell'ulteriore rischio (residuo) derivante dal fatto che lo stesso insieme di dati già anonimizzato è in circolazione.

Il terzo ricevente, dal canto suo, dovrà valutare non solo la tipologia di trattamento e le finalità che intende perseguire attraverso quelle informazioni, ma anche, nel limite del possibile, se il tipo di tecnica di anonimizzazione applicata dal titolare sia sufficientemente sicura rispetto al proprio contesto operativo. In particolar modo, dovrà porre attenzione alla "ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica",[190] giacché, come detto, l'irragionevolezza degli strumenti utilizzati è un fattore chiave

[188] *Ibid*., pp. 19 e 37-38. Dunque, malgrado la pubblicazione generale possa avere un impatto maggiormente incisivo sulla libera circolazione, in alcuni casi, la soluzione dell'accesso limitato potrebbe rappresentare il giusto compromesso capace di conciliare il monitoraggio del rischio con la libertà di disporre di informazioni essenziali per lo sviluppo della ricerca.
[189] CAVOUKIAN A., CASTRO D., *Big Data and Innovation, Setting the Record Straight*, *op. cit.*
[190] Gruppo di lavoro articolo 29, "*Parere 4/2007 sul concetto di dati personali*", *op. cit.*, p. 20.

nell'accertamento della disciplina nell'ambito della quale ricade chi è in possesso di tali informazioni.[191]

Se a seguito di queste valutazioni il rischio di reversibilità rimane inaccettabile, le parti dovranno decidere quale strada intraprendere tra la rinuncia a effettuare il trasferimento oppure l'esecuzione dell'operazione assicurando però il rispetto delle prescrizioni previste dal Regolamento generale sulla protezione dei dati personali.[192]

In ultima analisi, è doveroso precisare che, nonostante il cambio di paradigma illustrato sembri rispecchiare in maniera migliore la realtà odierna, il tema dell'anonimizzazione è lungi dall'essere prossimo ad una soluzione definitiva e condivisa. Il potenziamento della capacità di correlare informazioni provenienti da differenti risorse al fine di estrarre valore dai dataset sta mettendo sempre più in crisi la non personalità del dato anonimo,[193] tanto da spingere parte della dottrina a non considerarlo neanche più come un dato a carattere non personale.[194] Pertanto, non può escludersi che, in futuro, il legislatore europeo sarà costretto a riconoscere uno status "ibrido" – quasi personale – al dato sottoposto ad una corretta

[191] D'ACQUISTO G., NALDI M., *Big data e privacy by design*, *op. cit.*, pp. 36-37. In particolare: "In tal modo, se disponendo del dato anonimizzato e soltanto con l'ausilio di mezzi "irragionevolmente utilizzabili" è possibile identificare la persona, il dato anonimizzato non rientra nell'ambito di applicazione della legge".

[192] ICO, *Anonymisation*, *op. cit.*, p. 17.

[193] CALZOLAIO S., *Protezione dei dati personali*, in BIFULCO R., CELOTTO A., OLIVETTI M., (a cura di), *Digesto delle Discipline Pubblicistiche*, Utet giuridica, 2017, p. 606.

[194] ZENO-ZENCOVICH V., GIANNONE CODIGLIONE G., *Ten Legal perspectives on the "Big data revolution"*, in DI PORTO F. (a cura di), *Concorrenza e Mercato*, Numero speciale. Big Data e concorrenza, 2016, p. 34: "Now, one of the main scopes of data mining and data analytics is that of drawing inferences from data coming from the most diverse sources. Even though this data has been rigorously anonymized, and therefore should not fall under the GDP Regulation, once it is matched with other, equally anonymous data, it is possible — and often quite easily — to relate certain information to a specific person or to very small groups (e.g. a household). It would appear therefore that no data can be entirely anonymized, and therefore all data could be considered "personal" and therefore fall within the very strict rules of the GDP Regulation".

anonimizzazione, con una disciplina più stringente e più garantista rispetto a quella del dato non personale "puro".[195]

3.2 Il dato industriale e la questione della proprietà

Nella seconda categoria di dato non personale, ossia quella che, come detto, definiamo sinteticamente dati industriali o a-personali,[196] rientrano le informazioni che sin dall'origine non si riferiscono ad una persona fisica identificata o identificabile. Gli esempi che possono essere riportati interessano settori tra loro eterogenei: da alcune delle informazioni contenute nei documenti fiscali o contabili, ai dati provenienti da macchinari industriali o agricoli utili a migliorare la loro manutenzione o il loro impiego, fino a ricomprendere i dati relativi alle condizioni ambientali raccolti dai sensori presenti nel territorio. In aggiunta, considerata la definizione di dato personale fornita dal GDPR, possono considerarsi parte di questa seconda classe anche i dati relativi alle persone giuridiche.[197]

Anche il dato industriale, come quello anonimizzato, non è esente da problematiche la cui soluzione potrebbe cambiare radicalmente il mondo digitale come lo conosciamo oggi. In particolare, la questione che appare più pressante ed evidente concerne la qualificazione della situazione giuridica in cui versa colui che controlla tali informazioni: essendo al di fuori della sfera

[195] Lo stesso legislatore si dimostra aperto alla possibilità di riconsiderare questa fattispecie quando al considerando n. 9 del Regolamento 1807 afferma: "[…] Se i progressi tecnologici consentono di trasformare dati anonimizzati in dati personali, tali dati sono trattati come dati personali e si applica di conseguenza il regolamento (UE) 2016/679". Similmente, anche la Risoluzione del Parlamento europeo del 14 marzo 2017, Le implicazioni dei *Big Data* per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto, sembra paventare la possibilità che il dato non personale possa essere trattato alla stregua di uno personale nei casi in cui "l'uso dei dati non personali può ripercuotersi sulla sfera privata dei singoli o su altri diritti e libertà, con la conseguente stigmatizzazione di interi gruppi di popolazione".
[196] ELLIOT M. ET AL., *The anonymisation decision-making framework, op. cit*.
[197] *Supra*, par. 2.2, c).

del dato personale, tale soggetto non può essere qualificato come titolare del trattamento ai sensi del GDPR.[198]

È innegabile che l'attribuzione del titolo di proprietario ad uno dei numerosi soggetti coinvolti nella filiera del trattamento delle informazioni industriali, escludendo contemporaneamente gli altri dal godimento del medesimo beneficio, avrebbe delle conseguenze non indifferenti per le future prospettive della *data economy*. In tale ipotesi, emergono svariati interrogativi con riferimento al soggetto su cui ricade la responsabilità per la gestione di quei dati (ad esempio, in caso di re-identificazione), ai diritti che eventualmente possono essere attribuiti ad altri (come un diritto di accesso riconosciuto a chi ha contribuito alla creazione di quel dato o alle pubbliche amministrazioni) e, per quel che qui rileva, alla circolazione di questi dati che, mentre da un lato, rientrano in un differente regime giuridico rispetto ai personali, dall'altro, impongono comunque una valutazione dei rischi sottesi alla loro diffusione.

Negli ultimi anni vari autori si sono confrontati sul tema generalmente definito "*data ownership*", analizzando i vantaggi e gli svantaggi che potrebbero derivare dal riconoscimento normativo di un vero e proprio diritto di proprietà concernente il bene immateriale "dato". La progressiva separazione del dato dal tradizionale supporto fisico causata dalla diffusione dei sistemi di comunicazione e di archiviazione digitali ha sollevato interrogativi nuovi dal punto di vista del regime proprietario applicabile, a cui oggi non è stata ancora data una risposta condivisa.[199]

[198] Art. 4, punto 7), Regolamento (UE) 2016/679.
[199] GALIANO A., LEOGRANDE A., MASSARI S. F., MASSARO A., *I dati non personali: la natura e il valore*, in *Rivista italiana di informatica e diritto*, fasc. 1-2020, pp. 2-3.

Sebbene la questione si sia proposta anche con riferimento ai dati personali,[200] il carattere fondamentale del diritto sancito dall'articolo 8 della Carta di Nizza e le peculiari prerogative attribuite al *data subject* suggeriscono, quantomeno in questa fase ancora embrionale, di circoscrivere la valutazione della sostenibilità di un cambiamento di simile portata ai soli dati industriali.[201] L'incremento della quantità di questo tipo di informazioni avutasi con lo sviluppo della manifattura intelligente e delle tecnologie dell'informazione ha agitato il dibattito relativo alla qualifica del rapporto tra il detentore del dato industriale e il dato stesso, con particolare riferimento all'eventualità di riconoscere questo come titolare di un diritto di proprietà intellettuale.[202] Le caratteristiche che, ad oggi, contraddistinguono i dati, ossia l'immaterialità, la non rivalità e la potenziale escludibilità,[203] spingono l'interprete a

[200] Per alcuni riferimenti sul tema si rimanda a SCHWARTZ P., *Property, Privacy, and Personal Data*, in *Harvard Law Review*, 2004; AIELLO G. F., *La protezione dei dati personali dopo il Trattato di Lisbona, in Oss. del dir. civ. e comm., n. 2/2015,* p. 443; VICTOR J., *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, in *Yale Law Journal*, 2013; DREXL J., *Data Ownership and Access to Data. Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate* (documento redatto da DREXL J., HILTY R. M., DESAUNETTES L., GREINER F., KIM D., RICHTER H., SURBLYTĖ G., WIEDEMANN K.) 2016; PURTOVA N., *The Illusion of Personal Data as No One's Property*, in *Law, Innovation, and Technology*, 2015; TJONG TJIN TAI E., *Data ownership and consumer protection*, Tilburg Private Law Working Paper Series No. 09/2017.

[201] DREXL J., *Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy*, Max Planck Institute for Innovation and Competition Research Paper No. 18-23, 2018, pp. 23-25; DREXL J., *Designing Competitive Markets for Industrial Data – Between Propertisation and Access*, Max Planck Institute for Innovation & Competition Research Paper No. 16-13, 2016, pp. 60-61.

[202] DREXL J., *Designing Competitive Markets for Industrial Data*, *op. cit*., pp. 26-29.

[203] KERBER W., *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, Joint Discussion Paper Series in Economics by the Universities of Aachen, Gießen, Göttingen, Kassel, Marburg, Siegen, No. 37-2016, pp. 8-11.
L'A. precisa che mentre la non rivalità – ossia il fatto che il godimento del bene da parte di un soggetto non ne impedisca di per sé l'utilizzo da parte degli altri consociati ad un costo marginale pari a zero – è dovuta alla natura immateriale del dato; l'escludibilità, intesa come la possibilità di escludere gli altri dalla conoscenza di una determinata informazione, è resa possibile da misure tecniche (come la crittografia) che sono capaci di mantenere il dato segreto e dunque, essendo una questione prettamente empirica, potrebbe cambiare con lo sviluppo della tecnologia.

riconsiderare i tradizionali canoni su cui è stata costruita la dottrina del diritto di proprietà. Attualmente, stiamo fronteggiando una situazione mai vista prima: grazie ad un insieme di misure tecniche ed organizzative *ad hoc*, il detentore dei dati, nonostante non sia proprietario in senso giuridico e, di conseguenza, sia "mero possessore" del bene, riesce a comportarsi al pari di un vero e proprio titolare di un diritto di proprietà: può goderne e disporne liberamente – purché i dati siano non personali –,[204] può escluderne gli altri dal godimento e può procedere alla cessione a titolo oneroso. Oltretutto, a differenza di quanto accade per gli altri diritti di proprietà intellettuale tradizionalmente limitati nel tempo, questa "proprietà *de facto*" potrebbe essere mantenuta per un periodo potenzialmente illimitato.

3.2.1 Le soluzioni *de iure condito*: le normative vigenti

Prima di addentrarsi nel dibattito dottrinale concernente l'introduzione di un nuovo diritto esclusivo in materia di dati, si rivela opportuno valutare se gli strumenti giuridici attualmente a disposizione siano in grado di fornire una risposta immediata alle questioni suesposte.

Alla luce dell'evoluzione storica del *data law*, sembra opportuno iniziare dalla prima disciplina nel panorama europeo intenzionalmente dedicata alla tutela del patrimonio informativo: la Direttiva 96/9/CE relativa alla tutela giuridica delle banche di dati, in particolare focalizzandosi sul diritto *sui generis* sancito dal capitolo III. La struttura di tale prerogativa, specie nei termini definiti dalla giurisprudenza della Corte di giustizia, non sembra

[204] Se i dati a disposizione del titolare del trattamento fossero personali, egli non potrebbe disporne *ad nutum*, in quanto sottoposto all'obbligo di trattarli secondo le modalità previste dal GDPR e, soprattutto, nel rispetto dei diritti attribuiti al *data subject*.

collimare con una realtà in cui la stragrande maggioranza dei dati sono generati come sottoprodotto di altri trattamenti.[205] La scelta di circoscrivere la protezione normativa alla sola parte sostanziale del *database* e alle ipotesi in cui lo stesso viene ottenuto grazie a un investimento, qualitativamente e quantitativamente, rilevante da parte del costitutore al fine di organizzare i dati raccolti, escludendo pertanto i casi in cui la banca costituisca il frutto di un'attività creativa, rendono palese l'inidoneità del diritto *sui generis* a tutelare i singoli dati industriali generati nel contesto digitale.[206] Prendendo come riferimento il settore della *smart manufacturing*, le modalità di trattamento dei dati all'interno dell'impresa non implicano né un elevato investimento nella loro produzione, né una raccolta di elementi indipendenti sistematicamente o metodicamente disposti da fonti esterne, ricadendo conseguentemente al di fuori dell'ambito di applicazione della direttiva sulle banche dati.[207]

Peraltro, a fugare definitivamente ogni dubbio in merito, è intervenuta la Commissione europea che, con la recente proposta di Data Act, mira, per l'appunto, ad introdurre una disposizione di interpretazione autentica per mezzo della quale viene scongiurata l'applicazione del diritto *sui generis* alle banche di dati ottenuti dall'uso di dispositivi riconducibili all'ambito dell'*Internet of Things*.[208]

---

[205] *Supra*, cap. I, par. 4.

[206] Commission Staff working document, *Evaluation of Directive 96/9/EC on the legal protection of databases* (SWD (2018) 147 final), pp. 35-37.

[207] FIA T., *La tutela dei dati non personali: accesso, proprietà e regolamentazione*, in *Nuovo Notiziario Giuridico*, 2019, pp. 69-79.

[208] L'art. 35 della Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati), 23 febbraio 2022 (Com(2022)68 final) recita: "Il diritto "sui generis" di cui all'articolo 7 della direttiva 96/9/CE non si applica alle banche dati che contengono dati ottenuti o generati dall'uso di un prodotto o di un servizio correlato per non ostacolare l'esercizio del diritto degli utenti di accedere a tali dati e utilizzarli conformemente all'articolo 4 del

Allo scopo di proteggere il singolo dato in quanto tale si potrebbe, invece, fare ricorso alla tutela offerta dalla disciplina europea in materia di segreti commerciali.[209] Anche in tale ipotesi però, le caratteristiche dei dati industriali non permettono di soddisfare appieno i requisiti prescritti per beneficiare di tale protezione. L'intervento di una moltitudine di soggetti differenti nelle operazioni di produzione dei dati – chi detiene il macchinario su cui sono integrati i sensori, il produttore di tali sensori o chi progetta il *software* per il loro funzionamento – mette in discussione la possibilità di rispettare il requisito della segretezza delle informazioni, ossia la necessità che queste non siano generalmente note o facilmente accessibili.[210] In un contesto *data-intensive* non viene assolto in maniera adeguata neanche il secondo requisito, relativo al valore commerciale dell'informazione derivante dalla sua segretezza, poiché l'accertamento della rilevanza rivestita da un singolo dato spesso rimane oscuro oppure emerge solamente a seguito della combinazione con altri dati.[211] Oltretutto, è bene notare che la Direttiva sui segreti commerciali mira a tutelare il titolare del diritto dalle condotte illecite di quanti cercano di carpire informazioni protette e, pertanto, non attribuisce un'esclusiva paragonabile ad un vero e proprio diritto di proprietà.[212]

Sempre insistendo con le soluzioni già in campo, non ci si può esimere dall'ipotizzare un parallelismo con la proprietà privata tradizionalmente intesa, concernente i beni tangibili. Tuttavia, le

presente regolamento o di condividere tali dati con terzi conformemente all'articolo 5 del presente regolamento".

[209] Direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti (Gazzetta ufficiale n. L 157 del 15/06/2016).

[210] Art. 2, punto 1), lett. a), Direttiva (UE) 2016/943.

[211] DREXL J., *Designing Competitive Markets for Industrial Data*, *op. cit*. pp. 22-24.

[212] KERBER W., *A New (Intellectual) Property Right for Non-Personal Data?*, *op. cit.* p. 5.

differenze tra le caratteristiche dei beni fisici, sulle quali si fonda la proprietà civilistica, e quelle che contraddistinguono il dato sembrano troppo profonde per sostenere un'equiparazione efficace tra le due sponde.[213] In particolare, il carattere non rivale delle informazioni produce una differenza incolmabile rispetto al corollario fondamentale della proprietà fisica consistente nella potestà di impedire l'utilizzo da parte di altri membri della collettività della medesima risorsa. In aggiunta, la rilevanza dell'elemento della libera circolazione delle informazioni potrebbe prevalere sull'eventuale interesse legittimo del detentore a mantenere un dato nella propria esclusiva disponibilità. [214]

In conclusione, fra i diversi regimi disponibili nel quadro europeo nessuno è in grado di assicurare una protezione consona per i dati industriali nell'era della fabbrica intelligente. Ognuna delle singole soluzioni proposte si scontra con una peculiarità dei dati che contribuisce a definirli come un bene giuridico senza precedenti: la possibilità per il detentore di escludere *de facto* altri dal suo godimento senza che sia necessario fare ricorso ad una disposizione di legge. Tale aspetto spinge inevitabilmente ad interrogarsi sui benefici che potrebbero derivare dall'introduzione di un diritto proprietario specificamente dedicato ai dati non personali o da una differente regolazione dell'economia di tali informazioni.

3.2.2 La regolazione della *data economy* tra proprietà ed accesso

Il dibattito dottrinale vede ormai da tempo confrontarsi la fazione di coloro che premono per l'introduzione di un diritto di

[213] WIEBE A., *Protection of industrial data – a new property right for the digital economy?*, in *Journal of Intellectual Property Law & Practice*, 2016, p. 5.
[214] DREXL J., *Designing Competitive Markets for Industrial Data*, *op. cit.* pp. 26-29.

proprietà da attribuire ad uno o più dei soggetti che intervengono nella catena di trattamento del dato industriale, contro lo schieramento di chi preferisce affidarsi ai rimedi individuati di volta in volta dagli operatori di mercato in maniera autonoma, giacché una nuova privativa non farebbe altro che produrre effetti negativi per lo sviluppo dell'economia dei dati.

I primi si contraddistinguono per una concezione garantista nei confronti di alcuni degli attori coinvolti nella *data economy*. Il timore è che, limitando l'intervento del legislatore e lasciando che il mercato trovi da solo la soluzione ottimale, coloro che di fatto sono detentori di quantità massive di dati ottengano un potere contrattuale smisurato a discapito di quegli enti, pubblici o privati, che necessitano di tali dati per condurre le proprie attività. Secondo lo stesso ragionamento, la mancata previsione di un diritto di proprietà equivarrebbe all'attribuzione fattuale di tale diritto in capo all'industria dell'informazione.[215]

In realtà, sempre secondo i sostenitori di tale tesi anche lo sviluppo dell'economia dei dati trarrebbe enorme beneficio da un nuovo diritto di proprietà intellettuale, in quanto porterebbe ad una maggiore divulgazione delle informazioni tenute segrete, incrementando la trasparenza e, indirettamente, la capacità di innovazione, aiuterebbe a creare mercati per lo scambio di dati con conseguente allocazione ottimale delle risorse e diminuzione dei costi di transazione e, infine, impedirebbe agli sviluppatori di *software* di progettare macchine che, per garantire l'esclusività *de*

[215] PURTOVA N., *The Illusion of Personal Data as No One's Property*, *op. cit*. Nonostante l'analisi dell'A. sia circoscritta all'ambito dei dati personali, un ragionamento simile potrebbe applicarsi anche ai dati non personali, in quanto lo stesso meccanismo di raccolta delle informazioni e successiva esclusione degli altri dalla loro conoscenza, ipotizzato in tale contributo, può essere messo in pratica dai soggetti che producono *software* capaci di raccogliere e produrre dati, impedendo, al contempo, agli altri operatori la possibilità di fare altrettanto.

facto, rendono i dati non leggibili agli altri (a danno della portabilità e della libera circolazione delle informazioni).[216] In sostanza, questo diritto porterebbe ordine, eguaglianza e trasparenza in un mercato ancora disordinato.[217]

Dall'altra parte, la schiera dei detrattori accantona le motivazioni di giustizia sociale e preferisce fare ricorso ad argomentazioni prettamente economiche. Generalmente, affinché un diritto di proprietà intellettuale possa essere inserito nel tessuto economico è necessaria una giustificazione,[218] ossia un incentivo che spinga gli interessati ad investire nello sviluppo di un prodotto che altrimenti non verrebbe realizzato. Ora, se pensiamo alla *data economy,* è chiaro che il problema non è la sottoproduzione di dati: questi vengono generati e raccolti costantemente in quantità difficili anche da immaginare. Dunque, l'argomento principale è che questo mercato manca di una giustificazione tale da legittimare un'ingerenza così rilevante da parte dello Stato.[219]

Inoltre, sempre questo indirizzo insiste sulle numerose e forse insormontabili difficoltà che il legislatore dovrebbe risolvere nel caso in cui decidesse di introdurre una nuova privativa in un campo, quello del diritto di proprietà intellettuale, tradizionalmente caratterizzato dal principio del *numerus clausus*. Prima e forse più complessa fra tutte è la questione concernente il soggetto a cui dovrebbe essere attribuita la titolarità: nel *network* di imprese che intervengono durante il ciclo di trattamento del dato, non è agevole

---

[216] ZECH H., *A legal framework for a data economy in the European Digital Single Market: rights to use data*, in *Journal of Intellectual Property Law & Practice*, 2016.
[217] WIEBE A., *Protection of industrial data – a new property right for the digital economy?*, *op. cit.*, pp. 6-9.
[218] DREXL J., *Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy*, *op. cit.*
[219] KERBER W., *A New (Intellectual) Property Right for Non-Personal Data?*, *op.cit.*, pp. 8-9; DREXL, *Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy*, *op. cit*., pp. 16-17.

distinguere le operazioni di ciascuno e i diversi criteri di riconoscimento proposti non portano comunque ad una risposta chiara.[220] Per di più, come è stato attentamente osservato, non è da sottovalutare il rischio che una protezione del dato limitata al livello sintattico dell'informazione si propaghi poi anche a livello semantico, conducendo così ad un monopolio nell'informazione.[221]

Queste motivazioni spingono la maggior parte della dottrina ad insistere su una regolamentazione che, anziché introdurre un diritto di proprietà, disciplini l'accesso in modo tale da incentivare la libera circolazione delle informazioni.[222] Pertanto, la legge dovrebbe stabilire, da un lato, le condizioni che rendono illegittimo opporre un rifiuto all'accesso al proprio database quando sussiste un interesse pubblico alla condivisione e, dall'altro, predisporre un quadro giuridico volto a favorire la negoziazione fra le parti relativamente al prezzo da corrispondere a chi concede l'accesso.[223]

Nel panorama attuale, gli argomenti economici portati a sostegno della seconda soluzione hanno avuto maggiore forza persuasiva in dottrina. In effetti, lo sviluppo dell'era digitale, benché celere, è ancora agli albori ed un intervento così invadente da parte del legislatore appare quantomeno prematuro. Specialmente nel settore della *smart manufacturing* in cui i dati industriali rappresentano una risorsa non solo per chi produce il dato, ma anche per gli altri attori indirettamente convolti (ad esempio, i dati sulla

[220] *Ibid.*, p. 15; WIEBE A., *Protection of industrial data – a new property right for the digital economy?*, *op. cit.*, p. 8.
[221] KERBER W., *A New (Intellectual) Property Right for Non-Personal Data?*, *op. cit.*, p. 18; DREXL J., *Designing Competitive Markets for Industrial Data*, *op. cit.*, p. 13. È opportuno rammentare che, nella semiotica, viene delineata una distinzione fra il livello sintattico dell'informazione, che si riferisce alla rappresentazione della stessa per mezzo di segni e alle relative regole strutturali, e il livello semantico che, invece, concerne il significato che tali segni assumono.
[222] DREXL J., *Data Ownership and Access to Data.*, *op. cit.*, p. 9.
[223] DREXL J., *Designing Competitive Markets for Industrial Data*, *op. cit.*, pp. 55 e 62.

condizione delle strade raccolti dalle *smart cars* offriranno agli enti pubblici addetti alla manutenzione opportunità di intervento più accurate e tempestive).[224] Dunque, anche se la previsione di un diritto di proprietà permetterebbe virtualmente all'anello debole della catena di trattamento dei dati di avere maggior potere contrattuale, la libera circolazione di quegli stessi dati diverrebbe molto più lenta e farraginosa. In tal modo, la staticità derivante dall'introduzione di un diritto di proprietà intellettuale che risponde ad una concezione tradizionale di economia, mal si concilia con la dinamicità delle reti di valore tipiche della *data economy*.[225]

Al contrario, una disciplina volta a regolamentare l'accesso al fine di impedire alle aziende che detengono grandi quantità di dati di ostacolare la libera circolazione, è funzionale a stimolare la competitività tra imprese e ad offrire migliori opportunità di sviluppo. Significativo in tal senso è anche l'atteggiamento delle associazioni delle industrie più rappresentative che, nelle consultazioni promosse dalla Commissione europea, si sono sempre dimostrate contrarie all'introduzione di un diritto di proprietà, proprio perché ciò di cui necessitano non è tanto vedersi riconosciuta una nuova privativa, quanto, piuttosto, avere accesso ai dati detenuti da altri.[226] Difatti, la *big data analysis* è strettamente correlata alla quantità e, anzitutto, alla qualità dei dati che vengono impiegati quali input per l'analisi.[227] Per tale motivo, il vero vantaggio competitivo che contraddistingue un'impresa nella *digital economy* non risiede solo nel dataset posseduto, ma nel *software* di analisi, il quale,

[224] *Ibid.*, pp. 9-11; ZHANG S., *Who owns the data generated by your smart car?*, in *Harvard Journal of Law & Technology* Volume 32, Number 1, 2018, p. 300.
[225] DREXL J., *Designing Competitive Markets for Industrial Data*, *op. cit.*, pp. 16-18.
[226] *Ibid*., p. 5.
[227] D'ACQUISTO G., *Qualità dei dati e Intelligenza Artificiale: intelligenza dai dati e intelligenza dei dati*, in PIZZETTI F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, 2018, pp. 265-292.

invece, è suscettibile di protezione per mezzo della legislazione sul *copyright*.[228]

Evidentemente, l'impostazione che fa leva sull'incentivo all'accesso ai dati implica un aggiornamento della normativa che non sia limitato ad uno specifico settore, ma che, all'opposto, coinvolga in chiave organica tutte le branche del diritto che possono astrattamente toccare le modalità di accesso alle informazioni, come quelle in materia di concorrenza, di contratti e di segreti commerciali.

Infatti, per quanto riguarda il diritto *antitrust*, è doveroso sottolineare come l'accumulo costante e massivo di dati attuato dai *big players* che gestiscono le grandi piattaforme di internet rischi di mettere in pericolo il libero sviluppo di un mercato concorrenziale, contravvenendo alle regole sancite agli articoli 101 e 102 del TFUE.[229] In ragione di ciò, da più parti è giunto un monito volto ad evidenziare come le categorie impiegate attualmente dalla normativa *antitrust* (su tutte quella di "mercato rilevante")[230] non costituiscano più un argine significativo ai comportamenti di coloro che, proprio grazie alla quantità di dati a loro disposizione, sono già riusciti a consolidare una posizione di notevole vantaggio rispetto a tutte le altre controparti commerciali medio-piccole. Se l'introduzione di una privativa intellettuale non sembra una soluzione idonea,[231] anche una

[228] KERBER W., *A New (Intellectual) Property Right for Non-Personal Data?*, *op. cit.*, p. 10.; DREXL J., *Designing Competitive Markets for Industrial Data*, *op. cit.*, pp. 31-33.
[229] DREXL J., *Designing Competitive Markets for Industrial Data*, *op. cit.*, pp. 42-44.
[230] RUOTOLO G. M., *I dati non personali: l'emersione dei big data nel diritto dell'Unione europea*, in *Studi sull'integrazione europea*, 2018, pp. 100-105.
[231] DREXL J., *Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy*, *op. cit.*, p. 15: "If the legislature vested a data ownership right in the purchaser of a connected car, the manufacturer could not only request this purchaser to transfer or license the data ownership right. More importantly, the data ownership right would most likely fail to generate any additional income for the purchaser of the car since the manufacturer would immediately factor in the prospective payments made for the commercialisation of the data to the sales price for the car. In sum, the principle of freedom

semplice revisione "isolata" della disciplina della concorrenza potrebbe non essere sufficiente, giacché, malgrado le modifiche, la sua applicazione rimarrebbe ancorata alle categorie tipiche del diritto della concorrenza.[232]

Pertanto, un impianto regolamentare che abbia un impatto significativo non può prescindere da interventi congiunti sia nello specifico ambito del *data law*, sia in altri settori della disciplina europea. In primo luogo, quanto osservato dimostra che l'impostazione bipartita dell'ordinamento europeo non riesce a comprendere e regolare adeguatamente il fenomeno della digitalizzazione neanche con riguardo alla questione della proprietà del dato. In secondo luogo, sembra necessario che una riforma efficace arrivi ad inglobare, in primis, il particolare settore del diritto dei contratti, quantomeno al fine di estendere l'applicazione delle norme B2C anche alle piccole e medie imprese in tutti i casi in cui si trovino a trattare con i grandi operatori del mercato digitale,[233] e di stabilire un insieme di regole volte ad assicurare l'accesso ad informazioni essenziali nelle ipotesi in cui lo squilibrio di potere tra parte dominante e "nuovi consumatori" di dati non sia conciliabile in sede di negoziazione.[234]

Di nuovo, come verrà illustrato nel capitolo successivo, le argomentazioni testé esposte sembrano avere persuaso anche il legislatore continentale, il quale, con la recente proposta di Data Act, sembra intenzionato ad evitare un intervento troppo invasivo che,

---

of contract will always tend to allocate the economic value of using the subject-matter of protection according to the distribution of the bargaining power between the parties, irrespective of how property rights are allocated ex ante".

[232] DREXL J., *Designing Competitive Markets for Industrial Data*, *op. cit.*, pp. 47-53.

[233] FIA T., *La tutela dei dati non personali: accesso, proprietà e regolamentazione*, *op. cit.*, 2019, pp. 125-126.

[234] DREXL J., *Designing Competitive Markets for Industrial Data*, *op. cit.*, pp. 55-66.

allo stato attuale di crescita dell'economia dei dati, potrebbe rivelarsi prematuro e controproducente per il progresso della tecnologia.

4. Dagli insiemi di dati misti al "*Data by Design*"

Nel Regolamento sulla libera circolazione dei dati non personali trovano spazio anche le regole che stabiliscono la disciplina applicabile ai cosiddetti insiemi di dati misti,[235] ossia composti da dati sia personali che non. Come precisa la Commissione stessa,[236] la maggior parte delle raccolte di dati nella *data economy* è costituita da informazioni di natura eterogenea, poiché i sensori presenti sui dispositivi propri della *smart manufacturing* e dell'Internet delle cose (IoT) sono in grado di accumulare una miriade di dati senza alcuna distinzione con riguardo alla loro natura o provenienza. La *Guidance* della Commissione riporta esempi come i documenti fiscali di un'impresa, o un insieme che include sia dati statistici resi anonimi che dati non trattati inizialmente raccolti, oppure quando alcuni fra i dati raccolti da dispositivi IoT consentono l'identificabilità di una persona fisica.[237]

All'articolo 2, paragrafo 2 del RDNP è affidato il compito di trovare un equilibrio nell'applicazione della disciplina tra protezione del dato personale e libera circolazione di quello non personale. In particolare, la norma prevede che il Regolamento 1807 troverà applicazione solamente per la parte dell'insieme contenente i dati non personali. Sebbene astrattamente lineare, la soluzione prospettata dal legislatore europeo potrebbe rivelare alcune complessità sia nell'esecuzione che nel controllo. Nei fatti, il titolare

[235] La nomenclatura "insiemi di dati misti" è adottata dalla Commissione nella *Guidance*, p. 8, mentre il regolamento (UE) 2018/1807 fa riferimento a: "insieme di dati composto sia da dati personali che da dati non personali".
[236] Comunicazione della Commissione, *Guidance*, *op. cit.*, p. 8.
[237] *Ibid*., p. 9.

del trattamento è tenuto ad eseguire un'ulteriore operazione di scissione dell'insieme di dati in suo possesso se desidera usufruire, almeno per la parte costituita dai dati non personali, del regime meno restrittivo predisposto dal Regolamento 1807.[238]

Oltre alle difficoltà di procedere ad una corretta scissione derivanti dai problemi definitori descritti in precedenza, ci sono situazioni in cui effettuare la separazione dell'insieme di dati non solo non è economicamente conveniente, ma è addirittura tecnicamente impossibile. In siffatte ipotesi, sempre il paragrafo 2 dello stesso articolo prescrive che quando gli insiemi di dati sono "indissolubilmente legati", si applicherà solamente il GDPR a tutte le informazioni ivi contenute, "anche quando i dati personali rappresentano soltanto una piccola parte dell'insieme di dati". [239] Dunque, il Regolamento 1807 se, da un lato, statuisce un'estensione dell'ambito di applicazione della disciplina sulla protezione dei dati personali che, in questa particolare ipotesi, troverà attuazione anche nei confronti di un'informazione che non rientra nella definizione dell'articolo 4, punto 1) del GDPR; dall'altro, comporta anche una seconda e ulteriore restrizione alla libera circolazione del dato non personale, dopo quella della pubblica sicurezza.[240]

La Commissione ha chiarito che il concetto di insiemi indissolubilmente legati ricorre in quella situazione in cui "separarli sarebbe impossibile o ritenuto dal titolare del trattamento economicamente inefficiente o non tecnicamente realizzabile". [241]

---

[238] GRAEF I., GELLERT R., HUSOVEC M., *Towards a holistic regulatory approach for the European data economy*, *op. cit.*, pp. 6-7.
[239] Comunicazione della Commissione, *Guidance*, *op. cit.*, p. 10.
[240] Parere del Comitato economico e sociale europeo (CESE) sulla "Comunicazione della Commissione al Parlamento europeo e al Consiglio - Linee guida sul regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea" adottato il 25 settembre 2019, p. 8.
[241] Comunicazione della Commissione, *Guidance*, *op. cit.*, p. 10.

Dunque, salvo impossibilità tecniche o valutazioni economiche sfavorevoli, il titolare del trattamento si vedrebbe costretto ad effettuare la divisione del *dataset* nel caso in cui volesse svincolarsi dai doveri imposti dal GDPR.

Tuttavia, nella maggioranza dei casi, tale operazione comporta una diminuzione del valore dell'insieme e può anche rappresentare un costo non trascurabile, specie, si ripete, se si considera quanto sia arduo distinguere tra dato personale e non in alcune circostanze. Se a queste premesse aggiungiamo che non esiste una norma in nessuno dei due regolamenti che imponga la separazione dell'insieme ai titolari del trattamento, non possiamo che giungere alla stessa conclusione della Commissione europea: di regola, gli insiemi di dati misti saranno soggetti al regolamento sulla protezione dei dati personali.[242]

Da tale constatazione che, tra l'altro, solleva seri dubbi sull'opportunità di inserimento di una disposizione simile, nascono alcuni interrogativi in merito alla vera natura del Regolamento 1807. Concepito come ramo autonomo del *data law*, in quanto riferito ad una differente categoria di dato, le disposizioni che lo compongono contribuiscono a delinearlo – nella sostanza – come "costola" del GDPR. La conferma di siffatta ipotesi giunge dalla precisazione espressa dal Comitato economico e sociale europeo (CESE), il quale, preoccupato dal rischio che la "indissolubilità dei dati che sono al tempo stesso personali e non personali" possa condurre ad una loro "mercificazione più spinta", paventa la possibilità di procedere ad una unificazione dei due regolamenti, affinché "le norme del regolamento generale sulla protezione dei dati siano applicabili a tutti i dati e ai loro trasferimenti", mentre eventuali eccezioni

[242] *Ibid*., p. 11.

dovrebbero riguardare solamente "i "veri" dati non personali", intesa come categoria residuale riferita presumibilmente ai dati diversi da quelli anonimizzati.[243] Preoccupazione che, in parte, sembra riguardare lo stesso legislatore europeo quando all'articolo 8, par. 1, lettera a) del regolamento stabilisce che, nella valutazione dell'applicazione del nuovo regolamento che avrà luogo a distanza di quattro anni dall'approvazione, la Commissione dovrà porre attenzione "in particolare agli insiemi di dati composti sia da dati personali che da dati non personali, in considerazione degli sviluppi del mercato e dei progressi tecnologici suscettibili di ampliare le possibilità di de-anonimizzazione dei dati".

Al di là della questione relativa alla ridondanza dell'articolo 2, paragrafo 2 del Regolamento 1807, la classe degli insiemi di dati misti suscita alcuni interrogativi se collocata nel contesto dell'analisi dei dati.[244] Nonostante non sembri essere una situazione che si verifica di frequente, è possibile ipotizzare l'esistenza di attività commerciali in cui la separazione degli insiemi misti, non solo sia praticabile, ma addirittura sia vantaggiosa per il titolare del trattamento, in ragione del ritorno economico ricavabile dalla cessione dei dati non personali . Come è noto, l'amministrazione dei *dataset* non ancora separati, impone al titolare l'attivazione di tutte le misure tecniche ed organizzative atte ad assicurare la protezione dei dati a carattere personale, da individuare tramite una valutazione *a priori*, capace di declinare le prescrizioni generali del GDPR sulla situazione specifica *de qua*. Tuttavia, la circostanza che all'interno dello stesso complesso siano presenti anche informazioni a carattere

[243] Parere del CESE adottato il 25 settembre 2019, *op. cit.*, p. 8 e 12. Invero, con riferimento a questa ipotesi, parte dei votanti si è espressa in senso contrario, ritenendo che la diversità delle basi giuridiche dei due regolamenti non permettesse un'unificazione sul piano normativo, pp. 13-14.
[244] MONTAGNANI M. L., *La libera circolazione dei dati al bivio*, *op. cit.*, pp. 304-310.

non personale, le quali possono essere ricondotte nell'ambito di applicazione di un differente corpo normativo, suggerisce un passaggio dalla "semplice" *Privacy by Design* del GDPR,[245] ad una nuova "*Data by Design*": il precipitato logico derivante della sovrapposizione in capo ad un'unica entità della figura di titolare del trattamento dei dati personali e titolare dei dati non personali implica che il soggetto che vuole gestire separatamente i dati personali da quelli non personali dovrà dotarsi di una *policy* capace di individuare la natura dei dati a disposizione e di identificare i rischi derivanti dalla loro conservazione.

Tale *policy*, frutto dell'applicazione del principio di *Data by Design*, costituisce un modo – forse l'unico – per dare un significato all'articolo 2, paragrafo 2 del Regolamento 1807 e, conseguentemente, per rendere la gestione separata delle informazioni conforme alla legge. Difatti, la politica di amministrazione dei dati non dovrebbe riferirsi solo ed esclusivamente alle informazioni rientranti nel medesimo insieme di dati, ma, in chiave olistica, dovrebbe essere ritarata sulla base di tutti gli altri insiemi di dati a disposizione dello stesso soggetto. In buona sostanza, l'approccio basato sul rischio tipico della disciplina generale ritrova qui nuova linfa vitale, proprio perché tanto i dati anonimizzati quanto quelli industriali, se combinati insieme, possono tradursi in una re-identificazione della persona fisica anche se nessun dato apparentemente personale è stato coinvolto nel processo.[246]

Ad ogni modo, l'applicazione di queste "politiche di distinzione" tramite le quali è possibile sfruttare appieno i benefici

[245] CAVOUKIAN A., *7 foundational principles of privacy by design, op. cit*.
[246] Risoluzione del Parlamento europeo del 14 marzo 2017, Le implicazioni dei Big Data per i diritti fondamentali, *cit*.: "[…] che dall'impiego dell'analisi dei Big Data si osserva una confusione tra i dati personali e quelli non personali, il che può portare alla creazione di nuovi dati personali".

derivanti dall'economia dei dati, non può essere rimessa alla pura discrezionalità del soggetto che ricopre il ruolo di titolare del trattamento e titolare dei dati, il quale, abbandonato a sé stesso, rischierebbe di naufragare in un mare di indeterminatezza. [247] Pertanto, sembra che, ancora una volta, sia fondamentale il ruolo giocato dalle istituzioni pubbliche alle quali, di concerto con gli organismi di settore, spetta il compito di dare impulso ad un'iniziativa finalizzata all'adozione di linee guida che aiutino gli sviluppatori di servizi di gestione o analisi dei dati a programmare sistemi che siano in grado di riconoscere sapientemente il tipo di informazione raccolta o prodotta. A tale proposito, un nuovo versante nell'ambito dello sviluppo dell'intelligenza artificiale e del *machine learning* potrebbe riguardare proprio la progettazione di dispositivi e di *software* che nella fase di raccolta, analisi ed estrazione di dati abbiano la capacità di valutare la loro natura, per poi procedere al trattamento o alla collocazione nell'insieme confacente alle loro caratteristiche. Ad esempio, i macchinari impiegati nel settore della manifattura intelligente la cui funzione è quella di coadiuvare il lavoratore nello svolgimento dei propri compiti, dovrebbero applicare alla fonte una distinzione tra l'informazione relativa alla persona fisica che stanno assistendo, che chiaramente è a carattere personale, ed i dati che, invece, si riferiscono esclusivamente alla realizzazione del prodotto. In un certo senso, la *smart manufacturing*, terreno che più di ogni altro è interessato da tali sviluppi, riuscirà a soddisfare contestualmente sia la protezione dei dati personali del

[247] *Ibid*., il cui considerando "P" recita: "considerando che la proliferazione del trattamento e dell'analisi dei dati, l'elevato numero di soggetti coinvolti nella raccolta, nella conservazione, nel trattamento e nella condivisione dei dati e la combinazione di grandi insiemi di dati contenenti dati personali e non personali provenienti da una serie di fonti diverse, seppur generando opportunità significative, hanno creato una grande incertezza sia per i cittadini che per il settore pubblico e per quello privato relativamente ai requisiti specifici per la conformità alla vigente legislazione dell'UE in materia di protezione dei dati".

lavoratore che la libera circolazione delle informazioni industriali, se e solo se la sua realizzazione sarà accompagnata da una *policy* di *smart data by design*, ossia da una "intelligenza" applicata non solamente al processo produttivo rigorosamente inteso, ma anche alla gestione di tutti i dati che vengono generati all'interno dell'azienda la quale, in questo momento storico costituisce, peraltro, parte integrante di quel processo produttivo.

5. Verso la regolamentazione di un sistema integrato di gestione dei dati

All'impianto contintale va riconosciuto il ruolo di pioniere nella regolazione delle informazioni. L'Unione europea si è accorta per prima sia dell'esigenza di intervenire per limitare le possibili conseguenze dannose della datificazione, sia dell'essenzialità che il libero flusso delle informazioni ricopre per lo sviluppo economico e sociale di una società. D'altro canto, le questioni illustrate nel presente capitolo evidenziano l'incompiutezza del quadro regolamentare europeo. Le incertezze relative ai profili definitori e l'assenza di regole chiare con riguardo ai temi più complessi in materia di gestione dei dati testimoniano la necessità di un intervento per rivedere i profili che denotano maggiore debolezza dal punto di vista giuridico.

Parte della dottrina ritiene che il percorso verso una disciplina più adeguata al contesto attuale potrebbe persino passare attraverso un parziale superamento delle questioni di carattere definitorio.[248] Il tentativo dell'Unione europea di erigersi a paladina della tutela delle informazioni attinenti alle persone fisiche ha condotto ad un attaccamento quasi "morboso" alla nozione di dato personale,

[248] PURTOVA N., *The Law of Everything, op. cit.* pp. 79-80.

causando una iperestensione dell'ambito applicativo del GDPR che, nel lungo periodo, non è sostenibile. La staticità della soluzione interpretativa fornita dagli organismi europei non trova un solido appiglio in una ragionevolezza di utilizzo dei mezzi per re-identificare che non è mai uguale a sé stessa. Per tali motivi, le istituzioni continentali dovrebbero tornare a focalizzarsi maggiormente sul trattamento dei dati e sulle ripercussioni che questo potrebbe generare nei confronti della persona fisica.[249] Malgrado il diritto sancito dall'articolo 8 della Carta dei diritti fondamentali miri a tutelare dimensioni che fuoriescono dal più ristretto ambito della vita privata degli individui, una ricerca forsennata del dato personale, avulsa dalle circostanze in cui si inserisce lo specifico trattamento, si traduce in una "caccia alle streghe" caratterizzata da molta forma e poca sostanza.

Pertanto, le regole europee dovrebbero essere ridisegnate o, quantomeno, interpretate alla luce della *ratio* che sottende l'adozione delle discipline in materia di dati personali: proteggere l'individuo dal *vulnus* che potrebbe subire in ragione del trattamento delle informazioni che lo riguardano, garantendogli in tal modo la possibilità di sviluppare liberamente la sua personalità.[250] In tale direzione sembra dirigersi lo *use model* proposto in seno alla tavola rotonda organizzata dalla Organizzazione per la cooperazione e lo sviluppo economico nel 2014, secondo il quale la normativa a tutela dell'individuo dovrebbe trovare applicazione in tutti i casi in cui il trattamento sia suscettibile di incidere sulla persona fisica, indipendentemente dalla natura dell'informazione.[251]

---

[249] DALLA CORTE L., *Scoping Personal Data*, *op. cit*.
[250] KOOPS B.J., *The trouble with European data protection law*, in *International Data Privacy Law*, 2014.
[251] OECD, *Summary of the OECD privacy expert roundtable, Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*, 21-3-2014, pp.14-15.

Altrettante esigenze di riforma si palesano anche in riferimento ai dati a carattere non personale, specie in ragione dell'ambito applicativo eccessivamente ristretto del Regolamento 1807. Al di là delle lacune dal punto di vista definitorio, l'emanazione di un regolamento incentrato quasi esclusivamente sulla circolazione, nonostante la presenza di ulteriori aspetti di grande attualità e delicatezza, palesa un atteggiamento non adeguato, quasi pilatesco, da parte del legislatore continentale nei confronti di questa fattispecie.[252]

Particolare attenzione merita il dato anonimizzato, prima sottocategoria di dato non personale. È giunto per il legislatore il momento di affrontare il problema legato al costante rischio di re-identificazione, il quale non può essere azzerato se si vuole continuare a garantire una certa utilità al dato.[253] In virtù dello speciale rapporto di continuità che lega i dati anonimizzati a quelli personali, anche qui si rivela indispensabile un ripensamento in chiave contestuale e dinamica al fine di conciliare le esigenze di analisi dei dati con la tutela delle persone fisiche.[254] Il vizio originale dell'impostazione europea risiede nell'approccio esclusivamente scientifico-matematico con il quale sono state redatte le regole relative all'anonimizzazione. Per superare lo stallo venutosi a creare sarebbe opportuno implementare una disciplina che inglobi nella

[252] RUOTOLO G. M., *I dati non personali: l'emersione dei big data nel diritto dell'Unione europea*, *op. cit.*, p. 116.
[253] Problema che il legislatore ha dimostrato di recente di riconoscere, come sembra indicare il cons. n. 15 del Data Governance Act, nella versione approvata dal Parlamento, nella parte in cui afferma che: "Qualora la fornitura di dati anonimizzati o modificati non rispondesse alle esigenze del riutilizzatore, a condizione che siano stati soddisfatti i requisiti di svolgere una valutazione d'impatto in materia di protezione dei dati e consultare l'autorità di controllo ai sensi degli articoli 35 e 36 del regolamento (UE) 2016/679 e qualora i rischi per i diritti e gli interessi degli interessati risultino minimi, potrebbe essere consentito il riutilizzo in loco o remoto dei dati in un ambiente di trattamento sicuro".
[254] STALLA-BOURDILLON S., KNIGHT A., *Anonymous data v. Personal Data, op. cit.*, pp. 12-19.

valutazione dei rischi connessi all'anonimizzazione fattori sociologici e psicologici come la delicatezza del contesto in cui opera il detentore dei dati, il valore di tali informazioni e i motivi che potrebbero spingere gli *intruders* ad agire illecitamente al fine di appropriarsene.[255] La realizzazione di un'impresa di simile portata suggerisce un vero e proprio cambio di paradigma orientato ad una visione più ampia, non limitata ad un'ottica "dato-centrica" dove l'informazione isolata assume il ruolo di fulcro su cui si fondano le regole, ma, viceversa, estesa all'intero "*data environment*".[256] Solamente per mezzo dell'adozione del cosiddetto "*data situation approach*" è possibile includere tutte le variabili che hanno un impatto sulla qualificazione del dato e giungere ad una valutazione onnicomprensiva della natura dello stesso.[257]

Parimenti, la tematica del dato industriale esige particolare cautela, specie per la stretta relazione che lo lega alla libera circolazione dei dati e alla libertà di informazione. La recente genesi di tale figura, dovuta principalmente all'avvento della digitalizzazione, non consente di fare cieco affidamento sulla consolidata esperienza che appartiene alla categoria dei dati personali, i cui ricavati non si rivelano facilmente trapiantabili in un contesto giuridico in cui manca la dimensione relativa alla tutela di un diritto fondamentale individuale.[258] Ad ogni modo, la posizione

[255] OHM P., *Broken Promises of Privacy, op. cit.*, p. 1761.
[256] ELLIOT M., MACKEY E., *The Social Data Environment*, in O'HARA K., DAVID S. L., DE ROURE D., NGUYEN C. M-H. (eds.), *Digital Enlightenment Yearbook*, 2014, pp. 253-263.
[257] *Ibid*., pp. 38-41. In particolare, gli AA. Individuano quattro componenti nel *data envoronment*: 1) "*Data*", che comprende tanto i dati la cui natura deve essere ancora definita quanto quelli che possono vantare un legame reciproco; 2) "*Agency*", ossia i soggetti che possono accedere all'*environment*; 3) "*Governance process*", relativo alle regole, formali o fattuali, con che guidano gli utenti nella gestione dei dati; 4) "*Infrastructure*", intesa quale la struttura e i procedimenti che modellano il *data environment*.
[258] WIEBE A., *Protection of industrial data – a new property right for the digital economy?*, *op. cit.*

centrale che stanno acquisendo conduce a considerare i dati industriali come una vera e propria infrastruttura per la piena realizzazione del potenziale della *data economy*.[259] Se l'introduzione di un regime proprietario rema contro il libero flusso delle informazioni, in un mondo, quello attuale, in cui i dati sono diventati un fattore "essenziale" per l'esercizio di qualsiasi attività economica, appare allora indispensabile che il legislatore intervenga per regolamentare tale accesso, prevenendo la creazione di monopoli.[260] In tal senso, se, come dimostra la realtà dei fatti, coloro che già detengono grandi quantità di dati riescono ad impedire l'accesso altrui per mezzo di strumenti tecnologici che assicurano l'esclusività fattuale, il vantaggio competitivo che ne consegue andrebbe inevitabilmente ad alterare la libera concorrenza e lo sviluppo del mercato a livello non solo europeo, ma anche globale.[261]

La risposta a tutte le sfide collegate alla gestione dei dati esige un ulteriore passo in avanti da parte del legislatore e delle istituzioni europee tutte. Appare improbabile che una soluzione frammentaria ed eseguita per mezzo di interventi normativi diluiti nel tempo possa costituire un rimedio efficace. L'iperconnessione che caratterizza la realtà digitale richiede la creazione di un sistema continentale integrato di gestione dei dati dove la circolazione possa avvenire sulla base di regole comuni chiare, atte, da un lato, a costruire un modello di comunicazione e condivisione dei dati tra gli operatori, tanto pubblici quanto privati, che si svolga su un piano paritario; e, dall'altro, ad instaurare un clima di fiducia dove gli individui e gli utenti possano sentirsi al sicuro.[262] Il modo in cui l'Unione europea

[259] OECD, *Data-Driven Innovation*, *op. cit*., pp. 177-206.
[260] ABRAHAMSON Z., *Essential Data*, in *Yale Law Journal*, vol. 124, no. 3, 2014, pp. 867 e ss.
[261] GALIANO A. ET AL., *I dati non personali: la natura e il valore*, *op. cit*., pp. 11-15.
[262] OHM P., *Broken Promises of Privacy*, *op. cit.*, pp. 1759-1761 e 1767-1768.

deciderà di affrontare la prossima tappa avrà, probabilmente, un impatto ancor più rilevante di quanto accaduto con l'emanazione del Regolamento generale sulla protezione dei dati personali. Il vecchio continente, stretto dal potere "privato" degli OTT e da quello "pubblico" di altre superpotenze, rischia di perdere i vantaggi politici e tecnologici derivanti dalla gestione dei dati e, come naturale conseguenza, di abdicare definitivamente alla propria sovranità,[263] il cui mantenimento passa necessariamente attraverso la regolazione unitaria del fenomeno epocale della datificazione.

[263] OECD, *The Evolving Privacy Landscape*, *op. cit.*, pp. 9-12.

CAPITOLO IV

IL NUOVO MODELLO EUROPEO PER LA *GOVERNANCE* DEI DATI

Sommario:1. Introduzione. 2. Un nuovo modello "europeo" di *data governance* basato sulla condivisione dei dati. 3. Il potenziale impatto delle nuove normative sul diritto europeo dei dati. 3.1 Il riutilizzo dei dati "protetti" detenuti dagli enti pubblici e la seconda vita dei dati non personali. 3.2 Profili soggettivi del *data sharing* nel DGA. 3.2.1. Gli attori necessari e la persistenza dei problemi di qualificazione giuridica dei titolari dei dati. 3.2.2 Il ruolo caratterizzante dell'intermediario di dati nell'impianto europeo. 4. Spazio comune europeo di dati: *interdependence model versus independence model*.

1. Introduzione

I recenti sviluppi delle scienze tecnologiche hanno sollevato alcuni interrogativi in merito alla tenuta di un sistema giuridico fondato su una impostazione bipartita dei dati, in ossequio alla quale le informazioni vengono collocate in compartimenti separati e scarsamente comunicanti. Tale concezione si scontra con una diversa dinamica della circolazione dei dati, fortemente interconnessa e spesso non rispondente alle tassonomie previste dalle disposizioni normative. In ambito europeo, lo scollamento tra diritto e realtà produce un duplice risvolto negativo. Sul piano interno, le difficoltà applicative che derivano da simile regolamentazione si traducono inevitabilmente in un insufficiente sfruttamento delle possibilità offerte dal proprio patrimonio informativo, sia per gli organismi

pubblici che per i privati stabiliti nel territorio dell'Unione. Sul piano esterno, il medesimo ordinamento rende i dati "europei" facile preda per altre potenze, tanto occidentali quanto orientali), tecnologicamente più avanzate e affamate di informazioni. In tale contesto, l'assenza di infrastrutture e competenze adeguate, unita alle carenze normative illustrate in precedenza, apre la strada a forme legittime di appropriazione della ricchezza digitale del continente europeo da parte di soggetti esterni, ad esempio attraverso l'installazione di sistemi *hardware* e *software* facenti capo ad aziende private con sede al di fuori dell'Unione e, dunque, senza bisogno di ricorrere al compimento di azioni illecite riconducibili all'ambito della cybercriminalità.

Il pericolo di pagare a caro prezzo una sconfitta nella partita globale per la conquista della sovranità digitale ha spinto l'Unione europea ad intervenite nuovamente al fine di integrare il sistema normativo europeo in materia di dati. I provvedimenti maggiormente focalizzati sulla modifica del *data law* continentale, allo stato degli atti, non hanno ancora raggiunto la loro versione definitiva, ma dall'analisi delle azioni intraprese dalle istituzioni dell'Unione, ossia le "proposte" della Commissione, è possibile arguire la rotta che si intende percorrere. Nello specifico, sono in fase di discussione sia la Proposta per un regolamento concernente una nuova *governance* dei dati europea, sia la Proposta relativa ad un regolamento riguardante l'accesso e l'utilizzo dei dati. Per quanto riguarda il primo, il 25 novembre 2020 la Commissione europea ha pubblicato la proposta di regolamento in materia di *governance* dei dati, il cosiddetto Data Governance Act (DGA),[1] volto ad introdurre un modello di gestione dei dati che si discosti dalle altre realtà che al momento dominano lo

[1] Proposta di Regolamento del Parlamento europeo e del Consiglio relativo alla *governance* europea dei dati (Atto sulla governance dei dati), 25 novembre 2020 (Com(2020)767 final).

scenario internazionale. Le regole proposte tramite tale provvedimento mirano a realizzare un sistema capace di rilanciare l'industria continentale ed evitare di rimanere vittima di un neocolonialismo digitale.[2] Il 30 novembre 2021 il Parlamento europeo ed il Consiglio hanno raggiunto un accordo provvisorio e informale in merito alla proposta di DGA, successivamente approvato dal Parlamento in data 6 aprile 2022. La versione definitiva del testo e la successiva entrata in vigore attendono la formale approvazione da parte del Consiglio europeo.

In merito al secondo provvedimento, il 23 febbraio 2022 è stata pubblicata la "Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo", denominato Data Act (DA),[3] con l'obiettivo di fornire una prima soluzione alle questioni legate a quella particolare dimensione della *data ownership* trattata nell'ambito del terzo capitolo della tesi e consistente nella proprietà *de facto* che alcuni soggetti possono vantare sulle grandi quantità di dati. Pertanto, il Data Act è stato concepito allo scopo di garantire una migliore allocazione del valore delle informazioni tra i differenti attori che intervengono nelle *value chains* dell'economia dei dati,[4] con particolare riguardo alle informazioni generate o raccolte nel contesto dell'utilizzo di prodotti e servizi rientranti nell'ambito dell'*Internet of Things* o di servizi *cloud* e di trattamento dei dati generalmente intesi.

---

[2] IANNUZZI A., *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale*, in *Studi parlamentari e di politica costituzionale*, Anno 54, n. 209, 2021, p. 50.

[3] Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati), 23 febbraio 2022 (Com(2022)68 final).

[4] European Commission, Inception Impact Assessment, Ref. Ares(2021)3527151 - 28/05/2021.

In tal senso, tanto il DGA quanto il DA si pongono a ideale chiusura della presente tesi per un triplice ordine di ragioni. Innanzitutto, costituiscono i primi provvedimenti in cui, dopo la fondamentale dicotomia che ha segnato tutto il percorso di sviluppo del *data law* europeo, il legislatore decide di disciplinare unitamente entrambe le categorie di dati, pur mantenendo le stesse la propria autonomia all'interno dei regolamenti. In secondo luogo, entrambi gli atti permettono di comprendere se ed in che modo l'Unione europea si stia muovendo per trovare risposta alle questioni illustrate nei capitoli precedenti. Un sistema di *governance* capace di coniugare lo sviluppo della *data economy* con il valore primario della protezione dei diritti individuali è obbligato a confrontarsi con le istanze più impellenti che caratterizzano la materia dei dati, specie quelle definitorie, di re-identificazione e di titolarità. Infine, le proposte in esame si rivelano decisive per il futuro sviluppo del settore della manifattura intelligente. Nella mente del legislatore, la sovranità dell'Unione non rappresenta una questione di interesse prettamente pubblicistico, poiché si costruisce anche attraverso una "europeizzazione" del comparto industriale digitale. Ciò vale *a fortiori* in un contesto globalizzato in cui l'autorità dei Paesi sovrani viene costantemente e pesantemente messa in discussione dallo strapotere acquisito dalle compagnie private. La corretta implementazione di un approccio maggiormente comprensivo in materia di dati potrebbe rappresentare la strada maestra per realizzare un mercato più competitivo e una maggiore tutela delle persone giuridiche e, soprattutto, fisiche stabilite nell'Unione.

Da ultimo, va osservato che, in ragione della natura non definitiva dei provvedimenti in esame, il presente capitolo non comprenderà un'analisi puntuale delle singole disposizioni dei due testi, ma, per converso, verrà sviluppato con l'obiettivo primario di

individuare gli elementi dai quali è possibile desumere il modo in cui il diritto europeo dei dati sta (o non sta) evolvendo.[5] A tal fine, alla luce della maggiore risalenza e stabilità dovuta allo stadio di avanzamento della procedura di approvazione, il Data Governance Act verrà impiegato quale riferimento principale della presente disamina, mentre il Data Act verrà preso in considerazione nella misura in cui svela la linea predisposta dalla Commissione europea in materia di circolazione e di proprietà dei dati.

2. Un nuovo modello "europeo" di *data governance* basato sulla condivisione dei dati

Il DGA si inserisce nel solco delle proposte adottate dalla Commissione europea sul finire del 2020 allo scopo di riconfigurare il mercato unico europeo a seguito dei profondi cambiamenti causati dall'avvento della digitalizzazione.[6] Nello specifico, con il DGA la Commissione mira a rallentare la diffusione del cosiddetto "*Integrated Platform Model*" che costituisce il modello di trattamento di dati implementato dalle *big tech* e consolidatosi per lo più grazie ad una regolamentazione indulgente, se non del tutto

[5] La presente analisi assumerà entrambe le proposte adottate dalla Commissione europea quale punto di riferimento (Com(2020)767 final e Com(2022)68 final). Tuttavia, per quanto riguarda il Data Governance Act, richiamerà anche le versioni emendate del testo frutto dell'avanzamento del procedimento legislativo, qualora opportuno.

[6] Insieme alla proposta di DGA sono state pubblicate: la Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE (COM(2020) 825 final), noto come Digital Services Act; la Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali) (COM(2020) 842 final), meglio noto come Digital Markets Act. Per un approfondimento in merito, tra l'altro, ai profili relativi alla protezione dei dati personali interessati dal DMA, si veda: CONTALDI G., *Il DMA (Digital Markets Act) tra tutela della concorrenza e protezione dei dati personali,* in *Ordine internazionale e diritti umani,* n. 2/2021, pp. 292-308.

assente,[7] sostituendolo con un approccio che, per mezzo della regolazione prescrittiva, sia in grado di trovare il giusto equilibrio tra ruolo delle istituzioni pubbliche e tutela degli utenti, da un lato, e libertà d'impresa dei privati, dall'altro.

I tratti distintivi del modello europeo di *governance* dei dati sono stati individuati dal Garante europeo della protezione dei dati che lo ha descritto per mezzo di tre aggettivi: *open*, *fair* e *democratic*.[8] Per quanto riguarda il primo, la Proposta si lega senza soluzione di continuità a una politica di apertura dei dati non nuova all'ordinamento giuridico europeo. Già all'inizio degli anni Duemila, la Direttiva 2003/98/CE diede il via alle misure tese a promuovere il riutilizzo dell'informazione del settore pubblico. Di recente, questa normativa è stata abrogata per lasciare posto alla Direttiva *Open Data*,[9] che ribadisce il principio di *open by design and by default* per i dati in possesso del settore pubblico e amplia l'ambito soggettivo della direttiva.[10] La proposta di DGA si pone quale complemento della disciplina dal momento che il suo ambito oggettivo concerne quei dati che, benché in possesso delle pubbliche amministrazioni, sono sottoposti a speciali gravami giuridici che ne limitano la circolazione.[11]

---

[7] Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) (SWD(2020) 295 final), pp. 19-20.

[8] European Data Protection Supervisor (EDPS), *Opinion 3/2020 on the European strategy for data*, 16-06-2020, p. 2.

[9] Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (Gazzetta ufficiale dell'Unione europea, L 172, 26 giugno 2019).

[10] Art. 5, par. 2, Direttiva (UE) 2019/1024. Per un approfondimento, si veda: GOBBATO S., *Verso l'attuazione della direttiva (UE) 2019/1024 sul riutilizzo degli open data della PA: nuove opportunità per le imprese*, in *MediaLaws*, n. 2/2020, pp. 247 e ss.

[11] L'art. 3, par. 1 della Proposta di DGA recita: "Il presente capo si applica ai dati detenuti da enti pubblici, che sono protetti per motivi di: a) riservatezza commerciale; b) riservatezza statistica; c) protezione dei diritti di proprietà intellettuale di terzi; d) protezione dei dati personali".

Oltre che ad una interpretazione letterale,[12] l'aggettivo "*fair*" si presta ad una lettura più tecnica che rimanda all'accezione che il termine acquisisce, di regola, nel mondo dei dati, segnatamente ai cosiddetti FAIR *principles*. Benché originariamente concepita da un gruppo di *stakeholders* per migliorare la condivisione delle informazioni nel settore della ricerca scientifica,[13] questa esigua gamma di linee guida e *best practices* si è rivelata valida in tutte le occasioni in cui i dati rappresentano un *asset* fondamentale per lo svolgimento di attività commerciali e non commerciali. A riprova di quanto detto, lo stesso *explanatory memorandum* della Proposta per il DGA, laddove identifica espressamente i principi FAIR quale fonte di ispirazione per la bozza di regolamento, non fa altro che preconizzare un modello europeo dove i dati che circolano soddisfano le quattro caratteristiche che compongono l'acronimo FAIR: *findable* (reperibili), *accessible* (accessibili), *interoperable* (interoperabili), *re-usable* (riutilizzabili).[14] I primi due fattori sono strettamente interrelati poiché il primo mira ad incrementare la rintracciabilità dei dati attraverso l'impiego di identificatori unici e di metadati altamente descrittivi, mentre il secondo ambisce a migliorare la qualità dell'accesso ai dati mediante protocolli di autenticazione e autorizzazione capaci di garantire il rispetto degli obblighi giuridici in essere, dunque senza imporre necessariamente una politica di *open data*. L'interoperabilità è stata da tempo individuata quale strumento fondamentale per combattere la chimera

[12] Il significato letterale richiama un'idea di imparzialità ed equità e, pertanto, connota un sistema basato sul principio della non discriminazione. Tale principio rappresenta il cardine della disciplina europea in materia di accesso ai dati, il quale, assieme al principio di proporzionalità, è espressamente richiamato tanto dalla Direttiva Open Data (Artt. 8 e 11), quanto dalla Proposta di DGA (Artt. 5 e 11).
[13] WILKINSON M., DUMONTIER M., AALBERSBERG I. ET AL., *The FAIR Guiding Principles for scientific data management and stewardship*, in *Scientific Data*, 2016.
[14] Proposta di DGA, p. 2.

dell'assenza di standard comuni per i dati in ambito continentale: un ambiente digitale florido e dinamico non può prescindere dall'adozione di standard condivisi che permettano di rendere meno farraginoso il flusso dei dati tra i diversi anelli della catena di comunicazione.[15] Non a caso, la Proposta di Data Act dedica maggiore spazio rispetto a quanto fatto dal DGA al tema della interoperabilità, spingendosi sino alla previsione di norme prescrittive di carattere essenziale che i soggetti operanti nell'ambito del trattamento dei dati sono tenuti a rispettare.[16] Infine, il concetto di riutilizzabilità, ossia la possibilità di trattare i dati per una finalità diversa da quella originale,[17] costituisce l'obiettivo primario di tutto l'impianto regolamentare, poiché favorire l'incremento della ricchezza, della diversità e della qualità dei dati permetterà di cogliere al meglio i vantaggi offerti della *data-driven innovation*.

Da ultimo, fra le plurime interpretazioni che potrebbero fornirsi dell'aggettivo "*democratic*", la più calzante non può che essere quella che ne mette in risalto la differenza rispetto al tanto biasimato *Integrated Platform Model*. Come anticipato, il modello oggi predominante nella *data economy* consiste nella concentrazione di enormi quantità di dati nei *server* di pochi potenti attori le cui sedi sono collocate al di fuori dell'Unione. L'accumulo di potere che deriva da siffatto metodo di elaborazione dei dati costituisce un grave pericolo sia per la protezione delle persone fisiche con riguardo al trattamento dei loro dati personali,[18] sia per la concorrenza nel

[15] Per un approfondimento sul tema, si veda: KERBER W., SCHWEITZER H., *Interoperability in the Digital Economy*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (JIPITEC), *MAGKS, Joint Discussion Paper Series in Economics*, No. 12-2017.
[16] Capo VIII, Proposta di DA.
[17] DELOITTE, Realising the economic potential of machine-generated, non- personal data in the EU. Report for Vodafone Group, 2018, p. 5.
[18] Alcune fra le piattaforme digitali più note si sono rese spesso protagoniste di episodi di violazione della normativa a tutela dei dati personali. A titolo di esempio, si richiamano i

mercato europeo.[19] La volontà di prevenire il consolidamento dell'oligarchia dei giganti della tecnologia ha spinto, dunque, verso un modello improntato ad una logica spiccatamente redistributiva.[20] La divisione delle funzioni e la compartecipazione di più attori economici nella formazione delle catene di valore dei dati aspira a proporsi quale alternativa "più democratica" alla centralizzazione nella raccolta e nell'analisi dei dati delle grandi piattaforme online,[21] riducendo drasticamente le opportunità di concentrazione e, conseguentemente, la creazione di monopoli ed oligopoli.[22]

Anche in tale circostanza, la Proposta di Data Act fa proprio un principio evincibile dal DGA per tradurlo in disposizioni di carattere maggiormente prescrittivo e, al contempo, restrittivo. Nella Proposta più recente non mancano disposizioni che escludono *expressis verbis* dal novero dei beneficiari dei diritti e delle facoltà previste dal Data Act quelli che vengono designati dalla Commissione europea come "gatekeepers",[23] i quali, ricoprendo la posizione di soggetti che dettano le condizioni per l'accesso al

provvedimenti adottati dal Garante italiano per la protezione dei dati personali volti a sanzionare Facebook (Provvedimento del 10 gennaio 2019, Registro dei provvedimenti n. 5 (doc. web n. 9080914)) e Tik Tok (Provvedimento del 22 gennaio 2021, Registro dei provvedimenti n. 20 (doc. web n. 9524194)), o quello della Commission nationale de l'informatique et des libertés (CNIL) che sanziona Google (Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC).

[19] BAMBERGER K. A., LOBEL O., *Platform Market Power*, in *Berkeley Technology Law*, Journal 32, no. 3, 2017, pp. 1083-1087.

[20] Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal, *op. cit*. pp. 19-20.

[21] Con riguardo ai profili inerenti all'applicazione della normativa sulla protezione dei dati personali alle piattaforme, si veda: GARZONIO E., *Responsabilità degli ISP rispetto al trattamento automatizzato dei dati personali con finalità di comunicazione politica: applicabilità del GDPR alle piattaforme social*, in *MediaLaws*, n. 2/2019, pp. 190 e ss.

[22] *Ibid*. pp. 10-11.

[23] Art. 3 della Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali) (COM(2020) 842 final), meglio noto come Digital Markets Act.

mercato,[24] coincidono spesso con le *big tech* aventi sede in Paesi terzi. Nello specifico, in virtù di tale preclusione, i *gatekeepers* non possono vantare il medesimo diritto di accesso ai dati detenuti da altri attribuito dalla Proposta di DA alle compagnie operanti nel settore della gestione dei dati.[25]

Pertanto, al fine di massimizzare i benefici derivanti dallo sfruttamento diffuso del potenziale dei dati, il legislatore ha correttamente deciso di accompagnare la logica distributiva con una logica che potremmo definire collaborativa. Il *data sharing*, inteso quale strumento di politica economico-giuridica capace di incrementare il flusso di informazioni fra Stati membri e, di riflesso, l'accesso, funge da perfetto grimaldello per scardinare lo *status quo* in cui ristagna la *governance* dei dati attuale. La messa a disposizione volontaria da parte del detentore, direttamente o tramite un intermediario, in favore di soggetti esterni alla propria organizzazione assume una carica propulsiva enorme per la circolazione delle informazioni nel territorio europeo.[26]

La trasformazione dei dati da "sottoprodotto" del ciclo produttivo ad asset autonomo ha evidenziato la necessità di adottare politiche efficaci con riguardo alla loro condivisione. Il riutilizzo dei dati – ossia l'uso per una finalità diversa dalla originale – ha

[24] CONTALDI G., *Il DMA (Digital Markets Act) tra tutela della concorrenza e protezione dei dati personali*, *op. cit.*, p. 296.
[25] Art. 5, par. 2 e art. 6, par. 2, lett. d), Proposta di DA.
[26] Il fatto che la messa a disposizione sia volontaria, non implica necessariamente che la stessa debba in ogni caso essere gratuita. Anzi, soprattutto nel settore privato dove le disposizioni regolamentari non possono arrivare ad imporre un vero e proprio obbligo di *disclosure*, l'incentivo della remunerazione economica è assolutamente lecito, al pari di qualsiasi altro vantaggio, commerciale e non commerciale, di cui possa beneficiare l'ente privato disposto a condividere.
In aggiunta, dalla definizione di *data sharing* esula qualsiasi concessione di accesso che non risulti il frutto di una determinazione libera del detentore, sicché l'accesso dettato da provvedimenti delle autorità o per verifiche previste da disposizioni normative non potrà considerarsi come tale.

dimostrato di poter avere un valore e un impatto maggiori per la collettività, da un punto di vista sia economico che sociale, rispetto a quanto ne abbia l'utilizzo primario.[27] Al contempo però, proprio questa fondamentale capacità di analisi dei dati necessita di infrastrutture e di competenze che, spesso, non sono facilmente riscontrabili all'interno dell'ente che li ha raccolti e trattati in prima istanza.[28] Per tale motivo la condivisione può risultare uno strumento consono, specie se si considera che essa può interessare differenti soggetti a seconda del modello adottato. Il *data sharing*, infatti, può realizzarsi orizzontalmente quando avviene tra enti in concorrenza tra loro, in quanto operanti nello stesso mercato; verticalmente se intercorre tra organizzazioni che hanno già un rapporto di collaborazione, generalmente perché ricoprono posizioni differenti nella stessa filiera di produzione e distribuzione; esternamente nei casi in cui l'ente permette l'accesso ad operatori che si trovano al di fuori dal settore di mercato in cui agisce e che possono offrire un servizio sia su commissione di quest'ultimo che per interesse proprio.[29]

Le esperienze di *data sharing* già realizzate negli Stati membri hanno dimostrato di poter raggiungere benefici importanti sia dal punto di vista individuale, con maggiore visibilità sul mercato e riduzione dei costi di transazione per la singola impresa, che collettivo poiché fra le principali esternalità positive che si accompagnano ad una massiccia condivisione dei dati figurano un

[27] OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, Paris, 2019, p. 17.
[28] DELOITTE, Realising the economic potential of machine-generated, non- personal data in the EU, *op. cit*., p. 10.
[29] Altre distinzioni si basano sul grado di apertura consentito dal detentore dei dati – che può essere più o meno ristretto, sino ad arrivare alla modalità *open data* – oppure ai mezzi utilizzati, dal punto di vista sia giuridico (contratti di licenza), sia tecnico (API, piattaforme, *marketplace*, *algorithm-to-the-data*, *privacy-preserving computation*).

deciso passo in avanti verso la definizione di standard comuni europei, minori barriere in entrata ai mercati e una funzione di supporto essenziale per l'innovazione tecnologica.[30] Non è da sottovalutare neanche il potenziamento della sicurezza dei sistemi di gestione di dati: la condivisione delle informazioni relative agli attacchi informatici subiti permette a coloro che vi hanno accesso di ridurre le possibilità di successo delle violazioni effettuate con metodi analoghi, elevando in tal guisa il livello di protezione generale.[31]

Malgrado i benefici anzidetti, il *data sharing* fatica a decollare in ambito europeo. La realtà dei fatti restituisce uno spaccato in cui al timore di perdere vantaggi competitivi a causa della rivelazione di informazioni di carattere confidenziale o strategico, corrisponde uno smisurato accumulo di dati nei cosiddetti "*data silos*" dove ristagnano per un tempo indefinito senza essere condivisi con altri attori al fine di trarre beneficio dalla relativa cooperazione.[32] Al mantenimento di tale situazione anti-economica contribuisce un quadro normativo in materia di dati tuttora di ardua comprensione, specie con riguardo alla qualificazione della natura del dato, alle conseguenze derivanti dalla involontaria re-identificazione delle persone fisiche e al riconoscimento dei diritti spettanti a chi ha contributo alla creazione dell'informazione.[33]

Con particolare riguardo a tale ultimo profilo, il Data Act ricopre una funzione di completamento del DGA. La proposta più recente è stata concepita allo scopo di intaccare l'oligopolio

[30] Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal, *op. cit.* p. 15.
[31] OECD, *Enhancing Access to and Sharing of Data*, *op. cit.*, p. 45.
[32] WERNICK A., OLK C., VON GRAFENSTEIN M., *Defining Data Intermediaries – A Clearer View through the Lens of Intellectual Property Governance*, in *Technology and Regulation*, 2020, pp. 65-66.
[33] OECD, *Enhancing Access to and Sharing of Data*, *op. cit.*, pp. 70-71.

instaurato dai servizi OTT in ambito digitale, introducendo diritti di accesso e utilizzo dei dati generati tramite l'impiego di prodotti e servizi correlati. In sostanza, attribuendo il diritto di accedere ai dati agli utenti che proprio per mezzo delle loro azioni hanno contribuito alla produzione e raccolta di tali informazioni, il DA affronta con risolutezza le problematiche legate al consolidamento di una proprietà fattuale in capo a quei soggetti che per primi riescono a raccogliere informazioni tramite sistemi integrati, escludendo gli altri dall'accesso,[34] e impone obblighi di apertura che scattano al ricorrere di determinate condizioni.[35]

Dunque, è evidente che la proposta della Commissione riflette una presa di posizione ben precisa: di fronte all'alternativa illustrata nel capitolo precedente tra introduzione di un regime proprietario e promozione dell'accesso, l'Unione sembra schierarsi in favore del secondo approccio, in linea con quanto espresso dalla dottrina maggioritaria.[36] Siffatta scelta si fonda su due ragioni connesse, ma differenti. Da un lato, quella nota, concerne l'incentivazione di un regime concorrenziale e lo sviluppo di prodotti e servizi maggiormente innovativi; entrambi diretta conseguenza della aumentata disponibilità e circolazione dei dati. La seconda ragione, meno reclamizzata, ma costante immancabile tanto del DGA quanto del DA, coincide con l'opportunità di tenere lontane le compagnie extraeuropee, per mezzo di una politica di irrigidimento dei confini digitali del vecchio continente. La riprova di tale argomento perviene dallo stesso DA nella parte in cui, come anticipato, stante l'emersione di "un piccolo numero di imprese molto grandi con un

[34] In tal senso, il cons. n. 5 della Proposta di DA nella parte in cui afferma: "Il punto di partenza del presente regolamento è invece il controllo che il titolare dei dati effettivamente esercita, di fatto o di diritto, sui dati generati dai prodotti o dai servizi correlati".
[35] In particolare, artt. da 3 a 12, Proposta di DA.
[36] *Supra*, cap. III, par. 3.2.

notevole potere economico nell'economia digitale, ottenuto grazie all'accumulo e all'aggregazione di grandi volumi di dati e all'infrastruttura tecnologica per la loro monetizzazione", esclude dal diritto di accesso ai dati i *gatekeepers*.[37]

3. Il potenziale impatto delle nuove normative sul diritto europeo dei dati

In linea con la "Strategia europea per i dati" da cui discende,[38] la Proposta di Data Governance Act ha l'obiettivo di promuovere la creazione di uno "spazio unico europeo di dati" che consenta alle industrie continentali di rimanere competitive nell'era della digitalizzazione. Se durante i primi sviluppi dell'era digitale (Web 2.0) il nostro continente è rimasto a guardare mentre le altre potenze prendevano iniziativa, ora è arrivato il momento di superare gli ostacoli che ancora impediscono la piena realizzazione dell'immenso potenziale contenuto nelle informazioni generate dalle persone fisiche e giuridiche presenti in territorio europeo.[39]

Il termine *governance* è evocativo di una presa di coscienza da parte del legislatore delle difficoltà che si frappongono alla regolazione di un settore così complesso come quello dei dati. La costruzione di uno spazio dinamico e interconnesso per lo scambio, la circolazione e il conseguente sfruttamento del patrimonio digitale continentale richiede un approccio multidimensionale che affianchi alle disposizioni giuridiche, norme tecniche e organizzative capaci di modellare "procedimenti di condivisione, accordi e standard tecnici,

[37] Proposta di DA, cons. n. 36.
[38] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, "Una strategia europea per i dati" (COM(2020) 66 final).
[39] Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal, *op. cit.* p. 1.

fino all'istituzione di strutture e processi per la condivisione dei dati in modo sicuro, anche attraverso soggetti terzi".[40] Da ciò deriva anche una differente modalità di normazione dove, al classico metodo verticale puramente prescrittivo, viene anteposto un approccio collaborativo tra legislatore, settore privato e membri della collettività, al fine di consentire la maturazione di regole tarate in maniera più puntuale sul contesto di operatività dei soggetti coinvolti.[41]

L'intenzione di predisporre una normativa dedicata all'intero universo dei dati traspare in maniera chiara dal fatto che il Data Governance Act e il Data Act non fondano il proprio ambito di applicazione su una precisa tipologia di informazione come accaduto per i regolamenti precedenti. Prendendo come riferimento il DGA, il primo punto dell'articolo 2 della Proposta non fa riferimento ad alcuna distinzione nel momento in cui definisce i "dati" come: "qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva".[42]

A tale riguardo, malgrado la limitazione formale al dato informatico, il legislatore opta, di nuovo, per una definizione ampia e piuttosto generica. Se il termine "rappresentazione" rimanda al livello sintattico del dato, la "raccolta" potrebbe suggerire che, oltre alle informazioni in forma aggregata, la definizione faccia riferimento anche al livello semantico.[43] Ad ogni modo, l'esordio

[40] IANNUZZI A., *La governance europea dei dati nella contesa per la sovranità digitale*, *op. cit.*, p. 39.
[41] WERNICK A., OLK C., VON GRAFENSTEIN M., *Defining Data Intermediaries*, *op. cit.*, p. 66.
[42] La definizione è stata successivamente ripresa in maniera pedissequa dall'art. 2, punto 1) della Proposta di Data Act, il quale, pertanto, conferma l'approccio "unitario" inaugurato dal DGA.
[43] BALOUP J., EMRE BAYAMLIOĞLU, BENMAYOR A., DUCUING C., DUTKIEWICZ L., LALOVA T., MIADZVETSKAYA Y., PEETERS B., *White Paper on the Data*

dell'articolo 2 non implica affatto una commistione fra dati personali e non personali. Le due categorie non perdono la loro individualità e continuano ad essere sottoposte ad un regime giuridico differente, in virtù della asserita natura non riformativa del regolamento sulla *data governance* rispetto alle normative già vigenti nell'ambito del diritto dei dati.[44]

Ciononostante, è interessante notare come nell'elenco dell'originario articolo 2 del DGA figurasse la sola definizione di dati non personali. La scelta redazionale adottata dalla Commissione risulta singolare per un provvedimento in procinto di inserirsi in un impianto normativo basato su una marcata separazione. L'assenza di un riferimento alla categoria dei dati personali potrebbe riflettere l'idea, quantomeno della Commissione, che la disciplina delle informazioni a carattere personale sia ormai un assunto fondamentale dell'acquis comunitario tanto da rendere ultroneo qualsiasi richiamo in tal senso. Oppure, per converso, l'avvertita necessità di definire in maniera espressa la sola categoria dei dati non personali potrebbe evidenziare la scarsa considerazione di cui ancora gode questa fattispecie. Tale ultima lettura sembra, in un certo senso, confermata dalle parole riportate dal punto 3 dell'articolo 2, nel quale viene ripresa alla lettera la formulazione presente nel Regolamento (UE) 2018/1807, ma senza nemmeno menzionarlo. L'unico riferimento rimane il GDPR.

Orbene, questo passaggio, a prima vista innocuo, sembra celare e anticipare la volontà dei redattori del testo di intraprendere una parziale riforma della disciplina dei dati non personali. Il mancato richiamo alla fonte europea che per prima ha positivizzato

Governance Act, in *CiTiP Working Paper, KU Leuven Centre for IT & IP Law*, 2021, pp. 9-10.

[44] Proposta di DGA, cons. n. 3.

la definizione di dati non personali potrebbe riflettere la volontà della Commissione di assicurarsi una libertà di intervento maggiore al fine di colmare le lacune lasciate dal Regolamento 1807 a pochi anni di distanza dalla sua entrata in vigore.[45] Difatti, come si vedrà nel prosieguo, il proposito di non alterare le normative vigenti non impedirà alla proposta di DGA e a quella di DA di riscrivere alcune delle regole che disciplinano la circolazione dei dati non personali.

Peraltro, a seguito del monito del Comitato europeo per la protezione dei dati (EDPB) e del Garante europeo della protezione dei dati (GEPD) mosso dal timore opposto di modifiche surrettizie del sistema normativo a tutela dei dati a carattere personale,[46] il Parlamento europeo ha approvato l'aggiunta della definizione di dati personali.[47]

Malgrado l'ampiezza del suo spettro applicativo, il DGA non interviene direttamente in materia di tutela delle persone fisiche con riguardo al trattamento dei loro dati personali. In linea con la scelta dell'articolo 114 del TFUE come base giuridica, i meccanismi di *governance* che la proposta intende realizzare mirano essenzialmente a trarre massimo beneficio dalle potenzialità offerte dalla digitalizzazione del mercato interno senza per questo sacrificare la

[45] Se si eccettua il richiamo nel cons. n. 3 della Proposta di DGA, non compaiono altri riferimenti al Regolamento (UE) 2018/1807.

[46] Comitato europeo per la protezione dei dati (EDPB), Garante europeo della protezione dei dati (GEPD), Parere congiunto EDPB-GEPD 03/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati), Versione 1.1 del 9-06-2021, pp. 11-14.

[47] Il testo approvato dal Parlamento (European Parliament legislative resolution of 6 April 2022 on the proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act) (COM(2020)0767 – C9-0377/2020 – 2020/0340(COD); Ordinary legislative procedure: first reading) ha accolto quanto disposto nel Provisional Agreement resulting from interinstitutional negotiations relativo alla Proposta di DGA (COM(2020)0767 – C9-0377/2020 – 2020/0340(COD)) del 15-12-2021, il cui art. 2, *lett*. 2b) recita: "'personal data' means data as defined in point (1) of Article 4 of Regulation (EU) 2016/679".

concorrenzialità dello stesso.[48] Nella fattispecie, al fine di aggirare le barriere legali, commerciali, culturali e tecniche alle quali è ascrivibile la politica di *non-sharing by def*ault oggi dominante, il DGA si focalizza su specifiche situazioni la cui assenza di regolamentazione ha spesso condotto a soluzioni non ottimali o a squilibri di mercato. In primo luogo, punta ad incrementare il riutilizzo di quelle informazioni detenute dalle pubbliche amministrazioni che, in quanto gravate da diritti altrui, non sono sottoposte all'obbligo di divulgazione imposto dalla Direttiva *Open Data*.[49] In secondo luogo, la Commissione tenta di predisporre un meccanismo normativo teso a costruire un clima di fiducia nei confronti di chi svolge servizi di intermediazione dei dati, perno del sistema.[50] Infine, sempre in un'ottica di stimolo alla circolazione dei dati, il provvedimento introduce una nuova modalità di condivisione delle informazioni, denominata *data altruism*, consistente nella disinteressata messa a disposizione di dati personali da parte delle persone fisiche e di dati non personali da parte di quelle giuridiche in favore di soggetti pronti ad utilizzarli per finalità di interesse generale.[51]

In questo senso, il Data Act si pone sulla stessa lunghezza d'onda del DGA, giacché le sue disposizioni sono state concepite allo scopo di contribuire alla "creazione di un quadro di governance intersettoriale per l'accesso ai dati e il relativo utilizzo, disciplinando materie che riguardano le relazioni tra gli operatori dell'economia dei dati, al fine di fornire incentivi per la condivisione

[48] Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal, *op. cit.* pp. 17-18.
[49] Proposta di DGA, capo II.
[50] Proposta di DGA, capo III.
[51] Proposta di DGA, capo IV.

orizzontale dei dati tra i vari settori".[52] In sostanza, a fronte del medesimo obiettivo, il Data Act dedica le sue prescrizioni ad ambiti in parte diversi rispetto al DGA, nel tentativo di completare un disegno globale in materia di gestione dei dati da parte dei titolari e degli utenti collocati in territorio europeo. In particolare, il Data Act inserisce una nuova gamma di diritti e di corrispondenti doveri al fine di agevolare l'accesso ai dati da parte dei soggetti "più deboli" del ciclo di raccolta e trattamento e da parte di enti pubblici che potrebbero necessitare delle informazioni detenute dai privati in particolari situazioni emergenziali. Conseguentemente, la Proposta detta le condizioni e le modalità affinché i dati detenuti da chi fabbrica prodotti o offre servizi capaci di raccogliere e trattare informazioni siano messi a disposizione dell'utente o, su richiesta di quest'ultimo, di fornitori di servizi terzi, prescrivendo per diversi attori dell'attuale panorama dell'economia digitale nuove disposizioni in materia di trasferimento dei dati, validità delle clausole contrattuali e interoperabilità.[53]

[52] Proposta di DA, p. 2.

[53] La proposta di DA si distingue per la molteplicità di soggetti privati destinatari delle proprie disposizioni, i quali difficilmente sono sussumibili all'interno di una categoria unitaria. Il capo II, relativo alla "Condivisione dei dati da impresa a consumatore e da impresa a impresa" e il capo X dedicato alla norma di interpretazione autentica in materia di diritto "sui generis" della Direttiva 96/9/CE, sono rivolti ai soggetti che gestiscono i dati generati dall'uso di prodotti o servizi correlati, intendendosi come prodotto "un bene materiale e mobile, anche quando incorporato in un bene immobile, che ottiene, genera o raccoglie dati relativi al suo utilizzo o al suo ambiente e che è in grado di comunicare dati tramite un servizio di comunicazione elettronica accessibile al pubblico e la cui funzione primaria non è la conservazione e il trattamento dei dati" e come servizio correlato "un servizio digitale, anche software, incorporato in un prodotto o interconnesso con esso in modo tale che la sua assenza impedirebbe al prodotto di svolgere una delle sue funzioni", (art. 2, punti 2) e 3), Proposta di DA). Oltre a parte del capo II, il capo III, riguardante gli obblighi di messa a disposizione dei dati, è dedicato, in chiave generale, ai titolari dei dati, ossia alle persone fisiche o giuridiche che hanno "il diritto o l'obbligo, conformemente al presente regolamento, al diritto applicabile dell'Unione o alla legislazione nazionale di attuazione del diritto dell'Unione, o, nel caso di dati non personali e attraverso il controllo della progettazione tecnica del prodotto e dei servizi correlati, la capacità di mettere a disposizione determinati dati", (art. 2, punto 6), Proposta di DA). Il capo IV cambia ancora la natura del destinatario nella misura in cui dedica le norme circa le clausole abusive relative all'accesso ai dati alle

Alla luce di ciò, i paragrafi che seguono si focalizzeranno sugli aspetti delle due Proposte che potrebbero produrre un impatto rilevante nei confronti del diritto dei dati continentale attualmente vigente.

3.1 Il riutilizzo dei dati "protetti" detenuti dagli enti pubblici e la seconda vita dei dati non personali

La proposta di regolamento di DGA mira a completare la Direttiva *Open Data* attraverso un insieme di norme che, pur senza introdurre l'obbligo di autorizzare il riutilizzo,[54] ambiscono ad incentivare la condivisione e l'accesso alle informazioni rimaste al di fuori dell'ambito di applicazione di suddetta direttiva. Difatti, le pubbliche amministrazioni possono detenere informazioni su cui insistono diritti altrui e che, pertanto, non possono essere divulgate liberamente. Nello specifico, l'articolo 5 della Proposta individua come tali quei dati che necessitano di protezione per motivi di: a) riservatezza commerciale; b) riservatezza statistica; c) protezione dei diritti di proprietà intellettuale di terzi; d) protezione dei dati personali. In riferimento a tali informazioni, si contrappongono i

"imprese", che l'art. 2 definisce come "persona fisica o giuridica che, in relazione ai contratti e alle pratiche di cui al presente regolamento, agisce per fini connessi alla propria attività commerciale, imprenditoriale, artigianale o professionale", (art. 2, punto 8), Proposta di DA). I capi VI e VII, concernenti, rispettivamente, il passaggio ad un differente servizio e le garanzie per i trasferimenti internazionali di dati non personali, assumono come figura di riferimento i fornitori di servizi di trattamento di dati, dunque quegli operatori che offrono "un servizio digitale diverso da un servizio di contenuti online quale definito all'articolo 2, punto 5, del regolamento (UE) 2017/1128, fornito a un cliente, che consente l'amministrazione su richiesta di un pool scalabile ed elastico di risorse informatiche condivisibili di natura centralizzata, distribuita o altamente distribuita o un ampio accesso remoto allo stesso", (art. 2, punto 12), Proposta di DA). Infine, il capo VIII sull'interoperabilità ha come destinatari altrettanti soggetti, fra cui compaiono, assieme ai fornitori di servizi di trattamento dei dati, anche gli "operatori degli spazi di dati" e i venditori di "applicazioni che utilizzano contratti intelligenti", dunque di programmi informatici conservati "in un sistema di registro elettronico in cui l'esito dell'esecuzione del programma è registrato nel registro elettronico", (art. 2, punto 16).

[54] Art. 3, par. 3, Proposta di DGA.

diritti dei relativi titolari o dei *data subjects* e l'interesse, che nell'ottica del DGA assume rilievo preminente, al loro sfruttamento. Nel tentativo di individuare il giusto equilibrio, il legislatore interviene vietando gli accordi che, *de iure* o *de facto*, garantiscono un'esclusiva nell'utilizzo dei dati detenuti da enti pubblici o che comunque ne comprimono la disponibilità, salvi i casi in cui tali accordi rappresentino il modo migliore per generare benefici per la collettività.[55]

Successivamente, l'articolo 5, con riguardo alle condizionalità che gli enti pubblici possono imporre per l'accesso o il trasferimento dei dati protetti in loro possesso, tocca tre aspetti che assumono particolare rilievo nell'ambito del presente lavoro, specie in qualità di indicatori della direzione che sta prendendo l'ordinamento europeo dei dati.

In primis, il terzo paragrafo segnala la possibilità per l'ente pubblico di subordinare il riutilizzo dei dati ad un preventivo trattamento volto ad anonimizzare – o pseudonimizzare – i dati personali, oltre che a cancellare quelli riservati. In virtù di tale disposizione, comincia a guadagnare maggiore credito nel diritto eurounitario la validità delle procedure di anonimizzazione dei dati personali come misura applicabile dai titolari del trattamento al fine di tutelare le persone fisiche interessate,[56] sebbene il riferimento manchi di adeguato approfondimento dal punto di vista sia tecnico che giuridico. A conferma della rilevanza che sta gradualmente acquisendo tale meccanismo, anche l'opinione congiunta dell'EDPB e del GEPD accoglie con favore l'impiego dell'anonimizzazione come misura volta a tutelare i *data subjects* e, pertanto, rimarca la rilevante differenza, colpevolmente minimizzata dalla disposizione

[55] Art. 4, Proposta di DGA.
[56] Proposta di DGA, cons. n. 11.

in esame, che la separa dalla pseudonimizzazione.[57] Per giunta, il parere caldeggia l'inclusione esplicita di alcune fra le possibili misure segnalate nel capitolo precedente. In particolare, viene rivolto un invito ai redattori della disciplina a prevedere un obbligo di costante valutazione del rischio di de-anonimizzazione sotteso al trattamento e ad inserire apposite clausole volte ad imporre il divieto di re-identificazione dei dati anonimizzati nell'accordo di riservatezza che il riutilizzatore dovrebbe sottoscrivere al fine di prevenire la divulgazione di informazioni protette.[58]

Anche alla luce di tali osservazioni critiche, l'ultima versione emendata della Proposta di DGA sembra dedicare maggiore attenzione al tema. Oltre a non presentare più il riferimento alla pseudonimizzazione,[59] è previsto che il riutilizzatore si faccia carico degli obblighi di non re-identificazione, di implementazione delle misure tecniche ed operative per mantenere la de-identificazione e di invio di una notifica all'ente pubblico che ha concesso l'accesso in caso di avvenuta re-identificazione, la quale viene, in sostanza, equiparata ad un *data breach*.[60]

Peraltro, il provvedimento sembra introdurre un micro-regime normativo specificamente dedicato al trasferimento dei dati non personali "protetti" al di fuori dell'Unione; aspetto di cui, come detto, non vi è traccia nel Regolamento (UE) 2018/1807.[61] Il paragrafo 9 estende il principio di protezione equivalente, valevole per i dati personali, anche alle informazioni non personali che necessitano di una protezione rafforzata per ragioni di tutela della

[57] EDPB-GEPD, Parere congiunto 03/2021, *op. cit*., pp. 25-26.
[58] *Ibid.*
[59] Art. 5, par. 3, *lett*. a) del testo della Proposta di DGA approvato dal Parlamento europeo il 6 aprile 2022.
[60] Art. 5, par. 5 del testo della Proposta di DGA approvato dal Parlamento europeo il 6 aprile 2022.
[61] *Supra*, cap. II, par. 4.

proprietà intellettuale o dei segreti commerciali. Similmente a quanto accade per le decisioni di adeguatezza,[62] alla Commissione è conferito il potere di emanare "atti di esecuzione" per riconoscere la sostanziale equivalenza tra la protezione prevista dalla normativa del Paese destinatario e quella garantita dal diritto dell'Unione.[63]

L'articolato in esame procede poi con l'individuazione di una ulteriore categoria di dati non personali, definiti "altamente sensibili", in relazione ai quali la Commissione ha il potere di adottare "atti delegati" al fine di prescrivere particolari condizioni da osservare nelle ipotesi di trasferimento verso Paesi terzi. Prendono così forma nuovi obblighi di localizzazione dei dati, i quali possono oscillare dall'indicazione dei termini normativi e tecnici di trasferimento, alle limitazioni per il riutilizzo o per la trasmissione fuori dall'Unione, sino ad arrivare, in casi eccezionali, al divieto di trasferimento verso determinati territori.[64] Le informazioni rientranti in tale nuova classe di dati sono individuate da atti di natura legislativa emanati da organi dell'Unione volti a tutelare obiettivi di pubblico interesse. Rispetto all'unica eccezione della pubblica sicurezza prevista dall'articolo 4, paragrafo 1 del Regolamento (UE) 2018/1807, si assiste ad un evidente allargamento del novero degli interessi continentali che legittimano una restrizione alla libera circolazione delle informazioni, giacché le ipotesi riportate includono "la protezione della salute pubblica, l'ordine pubblico, la

[62] Art. 45, Regolamento (UE) 2016/679.
[63] Art. 5, par. 9, *lett*. a), Proposta di DGA. Tuttavia, nel caso in cui non sia previsto un atto di esecuzione della Commissione, il trasferimento è ancora possibile purché il riutilizzatore si impegni a rispettare gli obblighi di proprietà intellettuale, a non divulgare le informazioni in conseguenza del riutilizzo e ad accettare la giurisdizione dello Stato membro in cui ha sede l'ente pubblico interessato.
[64] Art. 5, par. 11, Proposta di DGA.

sicurezza, l'ambiente, la morale pubblica e la protezione dei consumatori, della privacy e dei dati personali".[65]

È interessante notare come nel complesso dei beni giuridici che i "dati non personali altamente sensibili" mirano a tutelare figurano anche quelli relativi alla persona fisica e ai dati che la riguardano. In questo senso, il DGA sembra dimostrare maggiore accortezza nella considerazione delle insidie per i diritti e le libertà delle persone fisiche che possono derivare dal trattamento di dati non personali. Difatti, le condizioni che la Commissione può applicare al trasferimento di tali dati dovrebbero essere parametrate sia sulla base dei rischi concernenti la sensibilità delle informazioni, che su quelli relativi alla re-identificazione dei singoli individui.[66] In sostanza, è proprio in questo passaggio che è possibile leggere un avanzamento della regolamentazione europea che, dopo alcune ambiguità, riesce finalmente ad integrare nel suo impianto anche i rischi sottesi al trattamento dei dati non personali.

Il nuovo quadro in materia di circolazione extraeuropea dei dati non personali viene completato – e rafforzato – da una norma di chiusura che gode di un ambito applicativo più vasto dell'articolo 5 testé illustrato, il quale rimane limitato ai dati non personali che cumulano i due requisiti della particolare "sensibilità" e della detenzione da parte di un ente pubblico. L'articolo 30 della Proposta di DGA mira a ridurre le occasioni di fuoriuscita dei dati non personali presenti nel continente prescrivendo, da un punto di vista generale, il dovere per i detentori di adottare tutte le misure tecniche, giuridiche e organizzative atte ad impedire il trasferimento, qualora

[65] Proposta di DGA, cons. n. 19. L'esempio di dettaglio che viene riportato dalla Proposta riguarda il settore sanitario dove "determinati set di dati detenuti da soggetti operanti nel sistema sanitario pubblico, quali gli ospedali pubblici, potrebbero essere considerati dati sanitari altamente sensibili".
[66] *Ibid.*

questo dovesse costituire un'operazione *contra legem* rispetto al diritto continentale.[67]

Peraltro, la richiesta di accesso a tali dati contenuta in una sentenza o in un provvedimento amministrativo può essere assecondata solamente se sussiste un idoneo accordo internazionale vigente tra il Paese del soggetto richiedente e l'Unione,[68] e, nel caso di potenziale infrazione delle norme vigenti negli Stati membri, esclusivamente qualora l'ordinamento giuridico del Paese terzo soddisfi determinate garanzie.[69] Oltretutto, prima delle modifiche intervenute con la versione più recente, tale ipotesi aveva portato ad un "surplus" di protezione dei dati non personali rispetto a quelli personali. La richiesta di parere preventivo alle autorità competenti che doveva essere effettuata dal destinatario del provvedimento per verificare la conformità del sistema giuridico del Paese terzo, costituiva un onere di cui non vi è traccia nella disciplina concernente il trasferimento dei dati personali.[70]

Successivamente, la proposta di Data Act non ha fatto altro che ribadire quanto disposto dal DGA in materia di trasferimento di dati non personali, indirizzando le medesime prescrizioni nei confronti di una particolare categoria della *data economy*: i fornitori

[67] Art. 30, par. 1, Proposta di DGA.
[68] Tale passaggio traspone fedelmente la disciplina in materia di dati personali, segnatamente l'art. 48 del GDPR, in quella relativa al trasferimento dei dati non personali.
[69] Art. 30, parr. 2 e 3, Proposta di DGA. In particolare, tra le condizioni che legittimano il trasferimento, il paragrafo terzo riporta: "a) il sistema del paese terzo richiede che siano indicati i motivi e la proporzionalità della decisione, e che l'ordinanza giudiziaria o la decisione, a seconda dei casi, abbia carattere specifico, ad esempio stabilendo un nesso sufficiente con determinate persone sospettate o determinate violazioni; b) l'obiezione motivata del destinatario è oggetto di esame da parte di un organo giurisdizionale competente del paese terzo; e c) in tale contesto, l'organo giurisdizionale competente che emette l'ordinanza o esamina la decisione di un'autorità amministrativa ha il potere, in virtù del diritto di tale paese, di tenere debitamente conto dei pertinenti interessi giuridici del fornitore dei dati tutelati dal diritto dell'Unione o dal diritto applicabile dello Stato membro".
[70] EDPB-GEPD, Parere congiunto 03/2021, *op. cit.*, pp. 49-51.

di servizi di trattamento di dati.[71] A tale riguardo, lo scopo della Proposta è dettato dalla volontà di aggiungere ulteriori garanzie contro il trasferimento di dati senza notifica da parte, in particolare, dei soggetti che offrono servizi di *cloud* ed *edge computing*, in ragione delle preoccupazioni relative all'accesso illecito da parte delle amministrazioni pubbliche di Paesi terzi.[72] A tal fine, la Proposta di Data Act si fa promotrice dell'introduzione di una politica di sicurezza anche per i dati non personali che i fornitori di servizi *cloud* ed *edge* dovrebbero implementare con l'obiettivo di impedire l'accesso ai sistemi in cui tali informazioni sono conservate.[73]

Sin dall'esame di queste prime disposizioni è possibile svolgere alcune considerazioni in merito alla forma che sta assumendo l'ordinamento europeo dei dati. Innanzitutto, è ravvisabile un parziale riequilibrio, che nel contesto europeo non sarà mai paritario, tra il peso che hanno i dati personali e quello che hanno i dati non personali, quantomeno in merito alla loro circolazione. Il cambiamento di impostazione, che si sostanzia nella trasposizione dei principi e delle regole stabiliti dal capo V del GDPR nel diverso ambito dei dati non personali, si manifesta in riferimento a quei dati che beneficiano di una disciplina più stringente in ragione della sensibilità degli interessi di rango costituzionale coinvolti. Il Regolamento 1807 adotta una prospettiva prettamente pubblicistica e interna, giacché consente una limitazione della circolazione di dati non personali in una dimensione intra-europea e per ragioni collettive attinenti a motivi di pubblica sicurezza. Al contrario, il Data

[71] Art. 27, Proposta di DA.
[72] Proposta di DA, pp. 3-4.
[73] Proposta di DA, cons. n. 78. In particolare, il testo fa riferimento a misure di sicurezza quali "la cifratura dei dati, la frequente sottoposizione a audit, l'adesione verificata ai pertinenti sistemi di certificazione della sicurezza e la modifica delle politiche aziendali".

Governance Act e il Data Act approntano una disciplina attenta al versante esterno dell'Unione e attribuiscono rilevanza anche agli aspetti privatistici coinvolti dalla gestione di dati non personali. Eloquente in tal senso il richiamo del DGA alla categoria dei dati non personali "altamente sensibili", che comprende informazioni inerenti ad interessi che vanno oltre la sfera della sicurezza pubblica, come la tutela del consumatore, dei dati personali e della privacy. Dunque, uno dei tratti caratterizzanti l'impostazione delle Proposte risiede in una maggiore consapevolezza del rischio sotteso al trattamento di dati non personali, sia perché il mantenimento della loro confidenzialità rimane necessario per salvaguardare la concorrenzialità delle imprese continentali, sia perché la loro combinazione e la loro analisi può sfociare nella re-identificazione della persona fisica.[74]

In aggiunta, adottando una chiave di lettura comparatistica, è possibile intravedere nel cambio di passo che la Commissione europea intende imprimere alla disciplina sul trasferimento dei dati non personali, una tenue somiglianza con l'impostazione assunta di recente dall'ordinamento dei dati della Repubblica popolare cinese.[75] A tale riguardo, la Cybersecurity Law of the People's Republic of China, nel 2017, e la Data Security Law of the People's Republic of China, nel 2021, hanno coniato due categorie di dati, rispettivamente gli "*important data*" e i "*core national data*",[76] le quali, assieme alle

[74] Proposta di DGA, cons. n. 19.

[75] Per un approfondimento in materia, si veda: LI Y., *Cross-border Data Transfer Regulation in China*, in *Rivista italiana di informatica e diritto*, fasc. n. 1/2021, pp. 67 e ss.

[76] Malgrado manchi nella disciplina di rango primario una vera e propria definizione di *important data*, gli atti normativi di rango secondario li descrivono come dati raccolti o generati all'interno della Cina, che non implicano il segreto nazionale, ma che sono strettamente correlati alla sicurezza dello stato, allo sviluppo economico o agli interessi pubblici. Questi possono comprendere anche dati di carattere personale.
Al contrario, l'art. 21 della Data Security Law definisce in maniera più puntuale i *core national data* come informazioni relative alla sicurezza nazionale, agli aspetti essenziali dell'economia nazionale e del sostentamento della popolazione ed agli interessi pubblici.

informazioni personali, devono sottostare a modalità di gestione alquanto restrittive in ragione del loro stretto legame con la sicurezza nazionale, lo sviluppo economico e gli interessi del Paese. Sebbene le misure di *data localization* non siano fra loro paragonabili,[77] le disposizioni europee in materia di trasferimento sembrano convergere, specialmente con riguardo ai dati detenuti dalle pubbliche amministrazioni,[78] verso la medesima meta del sistema cinese: una maggiore protezione del proprio patrimonio digitale dallo sfruttamento altrui e, poi, da potenziali ingerenze esterne.

Nella corsa verso l'acquisizione del potere derivante dai dati, stiamo assistendo ad uno scontro che si combatte, oltre che sul piano tecnologico, anche a colpi di atti normativi.[79] In questo senso, la

[77] L'art 37 della Cibersecurity Law impone ai "*Critical Information Infrastructure Operators*", ossia gli operatori che gestiscono strutture di rete o sistemi informatici particolarmente delicati per gli interessi del Paese, di conservare gli *important data* solamente all'interno del territorio della Repubblica popolare cinese. Per le ipotesi in cui dovesse rivelarsi assolutamente necessario, il trasferimento verso un altro Paese sarà possibile esclusivamente previo svolgimento di una valutazione di sicurezza secondo le indicazioni formulate dalle autorità deputate al controllo della cybersicurezza.
L'art 21 della Data Security Law prescrive misure ancor più stringenti per i *core national data*.

[78] A tale proposito si rinviene una differenza rispetto al sistema cinese. Mentre la categoria dei "dati non personali altamente sensibili" sembra essere al momento limitata ai dati detenuti dalle pubbliche amministrazioni, in quanto definita da una disposizione, l'art. 5, par. 11, rientrante nel capo relativo al "Riutilizzo di determinate categorie di dati protetti detenuti da enti pubblici", la normativa cinese assume, al contrario, carattere generale e, pertanto, non subisce limitazioni a seconda del soggetto che detiene i dati. Tale peculiarità rivela una significativa differenza tra la via "diretta" impressa dal legislatore cinese, il quale ha imposto prescrizioni restrittive a tutti i dati che possono assumere particolare rilievo per gli interessi nazionali prescindendo da qualsiasi distinzione sottostante, e quella prescelta dalla Commissione che attraverso interventi frammentati ha preferito intraprendere una strada più lunga e graduale.

[79] Per quanto riguarda il versante statunitense, assume particolare rilievo in tal senso il Clarifying Lawful Overseas Use of Data Act, noto come "Cloud Act", entrato in vigore nel 2018, il quale, al fine di agevolare le indagini delle autorità americane, impone agli *electronic communications services providers* e ai *remote computing service providers* di consentire l'accesso ai dati relativi agli utenti, indipendentemente dal luogo in cui tali informazioni sono localizzate, dunque, anche quando si trovano all'esterno degli Stati Uniti. Per un approfondimento, si vedano: CANTEKIN K., *Comity upon request. What does the new U.S. CLOUD Act tell us about the future of data flow regulation?*, in *Eurojus, Big data and Public Law: new challenges beyond data protection*, Numero speciale, 2018, pp. 79 e ss; CHRISTAKIS T., TERPAN F., *EU–US negotiations on law enforcement access to data:*

Proposta di DGA e quella di Data Act dimostrano di andare al di là del semplice rafforzamento del mercato unico, presentandosi come strumenti destinati ad incidere sulle sorti della sovranità continentale.[80]

3.2 Profili soggettivi del *data sharing* nel DGA

Focalizzando ora l'attenzione sul *data sharing*,[81] una adeguata comprensione del modello europeo non può prescindere da un'analisi del suo ambito soggettivo. A tale proposito, si possono distinguere le figure che ricoprono un ruolo imprescindibile, ossia i *data holders* (titolari dei dati) ed i *data users* (utenti dei dati), da quelle la cui presenza è solamente eventuale, ossia i soggetti che offrono servizi di intermediazione di dati, noti come *data intermediaries* (intermediari di dati). Malgrado il carattere accessorio, nel modello di condivisione dei dati in commento la funzione svolta dagli intermediari è destinata a diventare un elemento caratterizzante del sistema.

divergences, challenges and EU law procedures and options, in *International Data Privacy Law*, Vol. 11, No. 2, 2021, pp. 81 e ss.; BONCINELLI V., *Modelli tecnici e disciplina giuridica del c.d. cloud computing*, in *Rivista italiana di informatica e diritto*, fasc. n. 1/2021, pp. 34-38.

[80] IANNUZZI A., *La governance europea dei dati nella contesa per la sovranità digitale*, *op. cit.*, pp. 35-39.

[81] La disamina non avrà ad oggetto il *data altruism*, ossia l'ulteriore canale aperto dalla Commissione con il capo IV del DGA al fine di incentivare la circolazione delle informazioni convogliandole in grandi *pool* che fungano da carburante per un migliore sfruttamento del patrimonio digitale europeo. Il *data altruism*, massima espressione del principio di solidarietà nella *data economy*, consiste nella possibilità per le persone fisiche e per le persone giuridiche di, rispettivamente, acconsentire al trattamento dei propri dati personali o permettere l'utilizzo dei propri dati non personali, non per finalità individuali come avviene nello *sharing* tradizionale, ma nell'interesse della collettività, nel tentativo di produrre benefici diffusi per la società intera.

3.2.1 Gli attori necessari e la persistenza dei problemi di qualificazione giuridica dei titolari dei dati

Partendo dalle figure necessarie, il titolare dei dati coincide con la persona fisica o giuridica che "ha il diritto di concedere l'accesso a determinati dati personali o non personali sotto il proprio controllo o di condividerli".[82] Nell'ambito del ciclo di trasferimenti seguito dalle informazioni, il *data holder* incarna quel soggetto che ha la facoltà – giuridica o di fatto – di interrompere o reindirizzare il flusso dei dati, indipendentemente dal suo effettivo contributo dal punto di vista della raccolta o del contenuto dell'informazione.

In linea con quanto esposto nel capitolo precedente, il "titolare dei dati" del DGA coincide con quel soggetto che, nelle dinamiche della *data economy*, impone un approfondimento normativo in merito al rapporto giuridico che lo lega ai dati che si trovano nella sua disponibilità. Ciononostante, la Commissione rimane deliberatamente ambigua con riguardo all'approccio da seguire nella qualificazione di tale attore. Se il termine inglese "*holder*" suggerisce l'adesione a quello che è stato definito "*facts-based approach*", dove le nozioni di possesso o detenzione non assumono un rilievo *stricto sensu* giuridico, i diritti potestativi di concessione dell'accesso o di condivisione lasciano propendere per il contrapposto "*rights-based approach*". [83] Analoghe perplessità attengono alla versione italiana della proposta di DGA che riporta – forse poco opportunamente vista la terminologia impiegata nel GDPR – l'espressione "titolare dei dati". Sebbene il riferimento alla titolarità sembri indicare un'accezione di carattere giuridico, il mancato ricorso ad altre possibili traduzioni della parola *holder*,

[82] Art. 2, punto 5), Proposta di DGA.
[83] BALOUP J. ET AL., *White Paper on the Data Governance Act*, *op. cit*., pp. 10-13.

come "possessore" o "detentore", riflettono l'intenzione di astenersi da una presa di posizione precisa in merito al tema della *data ownership*.[84]

Ulteriori difficoltà nel corretto inquadramento della figura del *data holder* derivano dalla simultanea disponibilità di dati di carattere tanto personale quanto non personale. Con particolare riferimento ai primi, il Comitato europeo per la protezione dei dati si è speso per una modifica della definizione del titolare dei dati al preciso scopo di evitare qualsiasi formulazione che lasciasse presumere l'esistenza di un diritto di proprietà sui dati personali,[85] da parte sia del titolare del trattamento che dello stesso *data subject*.[86] Di conseguenza, il Comitato ha osservato che "piuttosto che fare riferimento a una persona giuridica che «ha il diritto di concedere l'accesso ai dati personali o di condividerli», la definizione di titolare dei dati dovrebbe, laddove conservata, fare riferimento al trattamento dei dati personali e alle relative condizioni conformemente al diritto applicabile in materia di protezione dei dati".[87] A tale riguardo, malgrado dettate da legittime preoccupazioni concernenti la tutela delle persone fisiche, le obiezioni del Comitato sembrano ancorate ad una visione anacronistica della realtà dei dati

[84] *Supra*, cap. III, par. 3.2.
[85] Comitato europeo per la protezione dei dati (EBDB), Dichiarazione 05/2021 relativa all'atto sulla governance dei dati alla luce degli sviluppi legislativi, adottata il 19 maggio 2021, pp. 5-6. Eloquente a tale riguardo il passaggio che recita: "le definizioni dell'atto sulla governance dei dati […] dovrebbero essere modificate per evitare incongruenze e incertezza del diritto ed essere in linea con la «natura dei diritti in questione», ossia il carattere individuale del diritto alla protezione dei dati personali come diritto di ciascuna persona e come diritto inalienabile, «al quale non è possibile rinunciare» e che non può essere reso oggetto di diritti di proprietà".
[86] Il testo approvato dal Parlamento in data 6 aprile 2022, che ha accolto le modifiche proposte nel Provisional Agreement del 15 dicembre 2021, recita all' art. 2, punto 8): "'data holder' means a legal person, including public sector body and international organisations, or a natural person who is not a data subject with respect to the specific data in question, which, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal data or non-personal data".
[87] EBDP, Dichiarazione 05/2021, *op. cit.* p. 6.

e, in tal senso, rischiano di rallentare il processo di mutamento che il *data law* europeo si accinge ad intraprendere sulla scorta dell'assunto secondo cui, nell'epoca della datificazione, non è più possibile proteggere le informazioni personali in assenza di una *data governance* adeguata. In particolare, le osservazioni non colgono appieno il passaggio concettuale insito nell'impianto del DGA dove la gestione dei dati, nata come costola della protezione delle informazioni a carattere personale, si amplia e diviene un corpo più grande che ingloba tutte le altre dimensioni legate al mondo dei dati, compresa la protezione di quelli personali da cui origina. Declinate nell'ambito soggettivo, le precisazioni del Comitato, intente a ricondurre le nuove categorie presenti nel DGA all'interno del quadro disciplinare della protezione dei dati personali, ostacolano uno sviluppo adeguato della nuova figura del *data holder*. In un contesto tecnologico dove il fattore che assume rilievo preminente consiste nella capacità di elaborazione dei dati indipendentemente della loro qualificazione all'origine come personali o non personali, il *data holder* riveste una posizione cruciale, per certi versi più rilevante di quella del titolare del trattamento del trattamento definito dal GDPR. Difatti, se un *data controller* (ossia un titolare del trattamento) è sempre un *data holder*, non è altrettanto corretto sostenere il contrario poiché un *data holder* non è sempre un *data controller*. È pertanto evidente che una efficace regolazione del trattamento dei dati non può che focalizzarsi, *in primis*, sul soggetto che si trova all'apice della *data economy*: il *data holder*.

Sotto il differente profilo della *data ownership*, la Proposta di DA sembra assumere un carattere maggiormente assertivo. In tal senso, il Data Act, nel tentativo di predisporre una possibile soluzione ad alcune delle questioni legate all'esercizio *de facto* di facoltà proprietarie sui dati, ha anteposto un approccio basato sul

diritto di accesso ai dati detenuti da altri all'introduzione di una privativa intellettuale vera e propria. Tenuto conto della non perfetta coincidenza terminologica tra i due atti, differentemente da quanto accade nel DGA, nel Data Act il titolare dei dati non è più inquadrato come attore che, per spirito di liberalità o vantaggio economico, mette a disposizione i dati in suo possesso in favore di soggetti terzi, ma, all'opposto, viene identificato come colui sul quale grava l'obbligo di garantire l'accesso qualora l'utente ne faccia richiesta.[88] Dunque, in attesa di successivi sviluppi, è già evidente che la Proposta più recente assumerà un punto di vista nuovo, parteggiando per gli attori che occupano una posizione di maggiore svantaggio nella catena di valore dei dati e che, pertanto, necessitano di un intervento normativo per prevenire il consolidamento di uno squilibrio deleterio per il progresso dell'industria e della società europee.[89]

Dal lato opposto, il titolo di *data user* spetta a quei soggetti che nel contesto del *data sharing* possono vantare un diritto di accesso sui dati detenuti dall'*holder* e che possono utilizzarli per finalità diverse, commerciali o non commerciali, rispetto a quelle per le quali erano stati originariamente raccolti.[90] Rientrano in tale definizione persone fisiche, enti pubblici, ricercatori, organizzazioni non governative e imprese operanti nello stesso o in un diverso settore rispetto al titolare,[91] i quali, mossi dallo scopo di estrarre valore aggiunto dai dati, sono i principali fautori dei benefici individuali e collettivi derivanti dalla condivisione.[92]

[88] Artt. 5 e 8, Proposta di DA.
[89] Proposta di DA, cons. n. 24.
[90] Art. 2, punto 6), Proposta di DGA.
[91] *Impact Assessment on enhancing the use of data in Europe*. Report on Task 1 – Data governance, prepared for the European Commission (SMART 2020/694 | D2), p. 40.
[92] OECD, *Enhancing Access to and Sharing of Data*, *op. cit.*, p. 35.

Per tale figura si presentano altrettante questioni riconducibili al differente regime giuridico che regola i dati personali e quelli non personali. L'utente dei dati che ha accesso ad entrambe le categorie di informazioni, oltre alla qualifica generale di *data user*, ricopre al contempo quella specifica di titolare del trattamento in relazione alla "quota" di dati personali cui ha accesso, in quanto anche la semplice consultazione rientra nelle operazioni definite dall'articolo 4, punto 2) del GDPR.[93] Malgrado ciò, la Proposta di DGA lascia senza risposta gli interrogativi in merito alla base giuridica su cui l'utente deve fondare le proprie operazioni di trattamento di dati personali.

Se il *data sharing* costituisce un meccanismo per rafforzare il mercato unico e per garantire il mantenimento della sovranità dell'Unione, l'attività del *data user* potrebbe essere equiparata al "compito di interesse pubblico" indicato dall'articolo 6, paragrafo 1, lettera e) del GDPR? [94] In tale ipotesi, proprio il DGA fungerebbe da atto del "diritto dell'Unione" necessario a stabilire la legittimità delle finalità perseguite dall'utente.[95] Il medesimo ragionamento vale per le categorie particolari di dati personali all'articolo 9 del GDPR, il trattamento delle quali può fondarsi su più di una base giuridica

[93] La disposizione citata classifica come operazioni di trattamento di dati personali "la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

[94] A tale proposito, risulta rilevante anche il considerando n. 45 del GDPR che, all'ultimo periodo, recita: "Dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire se il titolare del trattamento che esegue un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri debba essere una pubblica autorità o altra persona fisica o giuridica di diritto pubblico o, qualora sia nel pubblico interesse, anche per finalità inerenti alla salute, quali la sanità pubblica e la protezione sociale e la gestione dei servizi di assistenza sanitaria, di diritto privato, quale un'associazione professionale".

[95] L'art. 6, par. 3, del GDPR statuisce, infatti, che: "La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita: a) dal diritto dell'Unione; […]".

legata al soddisfacimento di motivi di interesse pubblico.[96] Queste ed altre questioni hanno spinto il Comitato europeo per la protezione dei dati (EDPB) ed il Garante europeo della protezione dei dati (GEPD) a sollecitare una modifica del testo licenziato dalla Commissione al fine di supplire alle mancanze dal punto di vista del coordinamento tra la Proposta di DGA ed il GDPR.[97]

3.2.2 Il ruolo caratterizzante dell'intermediario di dati nell'impianto europeo

L'intermediario di dati svolge la funzione di cerniera di collegamento tra i due attori necessari descritti in precedenza. Egli assume un ruolo che per certi versi appare paradossale. Sebbene la sua presenza sia meramente eventuale per il *data sharing*, che può prendere forma anche tramite la condivisione diretta tra *data holder* e *data user*,[98] il *data intermediary* ricopre una posizione decisiva all'interno del peculiare sistema europeo di condivisione dei dati in qualità di tassello aggiuntivo "capace di offrire un approccio

[96] In particolare, si fa riferimento alle lettere i) e g) del par. 2 dell'art. 9 del GDPR. Fra l'altro, appare pertinente anche la lettera j) del medesimo articolo, la quale rinvia all'articolo 89 del GDPR, in virtù dell'attività svolta dai centri di ricerca o di archiviazione e dagli istituti di statistica, per i quali la qualifica di *data user* potrebbe rivelarsi particolarmente calzante.
[97] EDPB-GEPD, Parere congiunto 03/2021, *op. cit*., pp. 11-14.
[98] L'art. 2, punto 7 della Proposta di DGA definisce in tal modo la "condivisione dei dati": "la fornitura di dati da un titolare dei dati a un utente dei dati ai fini dell'utilizzo congiunto o individuale dei dati condivisi, sulla base di accordi volontari, direttamente o tramite un intermediario".
Da un punto di vista tecnico, una delle modalità attraverso cui è possibile effettuare una condivisione di dati senza intermediario è rappresentata dal modello "*One-to-many data sharing*" che può attuarsi per mezzo di una *Application Programming Interface* (API) o tramite una apposita piattaforma realizzata dal *data holder* al fine di consentire l'accesso ai propri dati da parte di utenti esterni. Per un approfondimento, si veda: European Commission, Commission Staff Working Document "Guidance on sharing private sector data in the European data economy" Accompanying the document Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions "Towards a common European data space", (SWD(2018) 125 final), pp. 8-9.

alternativo all'attuale modello commerciale per le piattaforme tecnologiche integrate".[99]

Il compito principale svolto dal *data intermediary* è quello di agevolare l'incontro tra l'interesse del titolare dei dati a condividere e quello dell'utente dei dati ad avere accesso alle informazioni. In genere, rientra in tale categoria una gamma di soggetti del tutto eterogenea poiché le attività di intermediazione differiscono a seconda della clientela, del tipo di dati e dell'eventuale inclusione di servizi a valore aggiunto. Fra gli esempi più rilevanti nell'ambito della condivisione fra privati, meritano di essere menzionati i *data marketplaces* che raccolgono dati da numerosi *data holders* al fine di permettere il riutilizzo agli utenti, le *industrial data platforms* che offrono un ambiente virtuale sicuro e con regole comuni per lo scambio di informazioni tra le imprese partecipanti, i *personal information management services* (PIMS) il cui scopo principale è quello di garantire maggiore controllo e potere agli individui tramite mezzi tecnici che permettano di esercitare i diritti previsti da GDPR in maniera più effettiva e rapida, le *trusted third parties* dove l'intermediario ricopre l'incarico di ente certificatore con il compito di attestare la sussistenza di tutti i requisiti in materia, fra l'altro, di *privacy*, di sicurezza e di infrastruttura in capo alle organizzazioni partecipanti e, infine, le *data cooperatives* dove la gestione dei dati, specie personali, viene espletata al fine di riequilibrare l'asimmetria informativa che spesso pesa sui *data subjects* rispetto a chi tratta le loro informazioni.[100]

La forma adottata assume, dunque, particolare rilievo con riguardo ai servizi che l'intermediario è in grado di offrire poiché, oltre al *matchmaking* tra *holder* e *user* e alla certificazione

[99] Proposta di DGA, p. 6.
[100] *Impact Assessment on enhancing the use of data in Europe*, *op. cit*., pp. 38-40.

dell'avvenuta transazione, possono aggiungersi delle peculiarità capaci di rendere il *data sharing* estremamente appetibile per le imprese. Fra queste, degne di nota sono la predisposizione di clausole contrattuali standard, l'elaborazione dei dati al fine di convertirli in un formato comune o di anonimizzare informazioni personali o confidenziali, fino ad arrivare a servizi che consentono al titolare dei dati di mantenere un ampio controllo sulle informazioni condivise per mezzo di misure tecniche che garantiscono la conoscenza dell'identità di chi accede e le modalità con cui tratta i dati.[101] In tal senso, l'intermediario si caratterizza come quel soggetto che, anche ricorrendo ad apposite clausole *smart* di gestione dei dati,[102] mette a disposizione di titolari e utenti un sistema di *data governance* che, grazie alla conformità alla normativa europea conferitagli per impostazione predefinita, consente un flusso massivo, in entrata e in uscita, di informazioni essenziali per le politiche pubbliche, le attività di impresa e lo sviluppo della ricerca.

Ad ogni modo, malgrado non risultino ancora ben definiti i contorni della figura disegnata dalla Commissione, dalle disposizioni proposte traspare una versione "europea" di intermediario contraddistinta da una libertà di azione piuttosto circoscritta, specie in virtù dell'introduzione di un obbligo di neutralità.[103] In ossequio a tale prescrizione, il *data intermediary* deve limitarsi ad instaurare una connessione tra *holder* e *user*, senza poter poi utilizzare i dati che entrano in suo possesso per finalità diverse dal semplice *sharing*.

[101] European Commission, Commission Staff Working Document "Guidance on sharing private sector data in the European data economy", *op. cit.*, p. 11.
[102] Per un approfondimento in merito alle implicazioni giuridiche legate alla diffusione degli *smart contracts*, si veda: BOMPREZZI C., *Implications of Blockchain-Based Smart Contracts on Contract Law*, *Luxembourg Legal Studies*, Vol. 23, Nomos, 2021, in particolare pp. 47-73.
[103] CALOPRISCO F., *Data Governance Act. Condivisione e "altruismo" dei dati*, in *Associazione Italiana Studiosi di Diritto dell'Unione europea* (AISDUE), *Focus "Servizi e piattaforme digitali"*, n. 3, 2021, p. 68.

In primo luogo, tale aspetto implica che, se un'organizzazione desidera operare in qualità di *data intermediary* in aggiunta ad altri servizi già parte della sua offerta, dovrà necessariamente procedere in via preventiva ad una separazione strutturale del proprio organigramma.[104] Prescrizioni di questo tenore mirano ad evitare la comparsa di conflitti di interesse fra gli intermediari che potrebbero sfruttare la loro posizione di privilegio per entrare nel mercato in cui operano i titolari e gli utenti. In secondo luogo, la neutralità esige l'applicazione del principio di non discriminazione che impedisce differenze di trattamento basate sul tipo di *holder* o *user* interessato a partecipare (*opennes obligation*),[105] o sul contenuto dei dati trattati (*zero knowledge platform approach*), salvo un controllo, seppur limitato, ai fini di prevenzione di condotte criminali che potrebbero consumarsi per il tramite dell'intermediario.[106]

Da tali osservazioni si deduce che l'intermediario europeo dovrebbe assumere un atteggiamento piuttosto "passivo", facendo da ponte tra titolare ed utente per mezzo dell'infrastruttura e dei mezzi per effettuare lo scambio di dati, ma senza privilegiare i propri interessi o quelli di alcuni solamente fra i partecipanti. Per tale ragione, pur rientrando nella definizione generale di intermediario, non sono considerati tali alla luce del DGA quelli che servono gruppi chiusi di *holder* e *user*, i fornitori di servizi *cloud* e i *data brokers*, poiché aggregano e trasformano i dati per poi fornire un servizio autonomo agli utilizzatori, senza che si instauri alcun rapporto con i titolari originari. [107] Un'eccezione all'imparzialità intesa quale

[104] Proposta di DGA, cons. n. 26.
[105] Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal, *op. cit.* pp. 25-27.
[106] Questo è quanto emerso durante le consultazioni preliminari. A tal proposito, si veda il *Workshop on labels for or certification of providers of technical solutions for data exchange: Summary of discussions*, del 12-05-2020, pp. 2-4.
[107] Proposta di DGA, cons. n. 22.

corollario dalla neutralità ricorre, tuttavia, in quelle ipotesi in cui gli intermediari gestiscono dati a carattere personale allo scopo di agevolare l'esercizio dei diritti riconosciuti agli individui dal GDPR e, dunque, nell'interesse di questi.[108]

Dalla lettura dell'articolo 11 sorge il sospetto che la figura del *data intermediary* sia stata progettata in modo forse troppo restrittivo. Similmente alla contrapposizione tra *privacy* e *utility* illustrata da Ohm nel contesto delle procedure di anonimizzazione,[109] anche in tale ipotesi si instaura una antitesi tra *neutrality*, da un lato, e *utility*, dall'altro. Una concezione troppo stringente del requisito di neutralità si traduce in uno spettro di possibilità assai limitato per l'intermediario, il quale deve attenersi alla semplice agevolazione dello scambio dei dati nel formato in cui li riceve dal titolare e alla conversione in formati specifici "solo allo scopo di migliorare l'interoperabilità a livello intrasettoriale e intersettoriale".[110] Dunque, da un'interpretazione letterale, sembrerebbe che al *data intermediary* siano preclusi quei trattamenti che alterano le informazioni, anche quando diretti a de-identificarle. In tal modo, si rischia di spegnere sul nascere uno degli sbocchi più promettenti dei servizi di intermediazione, ossia la creazione di un soggetto interposto che, applicando meccanismi generali di *governance* consistenti in forme massive di anonimizzazione preventiva,

[108] Il cons. n. 23 della Proposta di DGA identifica questi intermediari come "categoria specifica", in quanto "[t]ali fornitori si concentrano esclusivamente sui dati personali e cercano di rafforzare la capacità di agire e il controllo dei singoli individui in merito ai dati che le riguardano. Assisterebbero i singoli individui nell'esercizio dei loro diritti a norma del regolamento (UE) 2016/679, in particolare gestendone il consenso al trattamento dei dati, il diritto all'accesso ai propri dati, il diritto alla rettifica dei dati personali inesatti, il diritto alla cancellazione o "diritto all'oblio", il diritto a limitare il trattamento e il diritto alla portabilità dei dati, che consente agli interessati di trasferire i propri dati personali da un titolare del trattamento a un altro".

[109] OHM P., *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, UCLA Law Review, Vol. 57, 2010, pp. 1701 e ss.

[110] Art. 11, par. 4, Proposta di DGA.

eviterebbe all'utente dei dati l'assunzione della qualifica di titolare del trattamento ai sensi del GDPR. Sulla scorta delle considerazioni in merito alle potenziali storture derivanti da siffatta formulazione, gli emendamenti inseriti nell'ultima versione della Proposta di DGA includono le procedure di de-identificazione fra i servizi aggiunti che l'intermediario può includere nella sua offerta.[111] Del resto, diversamente opinando il DGA potrebbe rivelarsi velleitario nella misura in cui si fonda su una neutralità utopica: la previsione di obblighi esageratamente rigidi in ossequio alle esigenze di neutralità corre il pericolo di rendere poco appetibile un settore di mercato in cui gli operatori che auspicabilmente potrebbero occuparlo devono possedere delle capacità di investimento e delle *expertise* tali da garantire la gestione continuativa ed efficace di un sistema che si prospetta incredibilmente complesso e di ampia portata.

Infine, analogamente a quanto accade in merito al riutilizzo dei dati degli enti pubblici, è opportuno notare che anche con riguardo ai servizi di intermediazione si intravede una modesta rivalutazione della fattispecie dei dati non personali. L'articolo 11, nella sua versione originale, prevede che l'intermediario adotti misure tecniche, giuridiche e organizzative sia per impedire l'illegittimo accesso o trasferimento di dati non personali,[112] sia per garantire un elevato livello di sicurezza per la conservazione e la trasmissione di tali dati.[113] Pertanto, assistiamo di nuovo ad una riproduzione degli istituti tipici del GDPR, nella specie il principio

[111] L'art. 12, lett e), del testo della Proposta di DGA approvato dal Parlamento europeo il 6 aprile 2022, recita: "data intermediation services may include offering additional specific tools and services to data holders or data subjects for the specific purpose of facilitating the exchange of data, such as temporary storage, curation, conversion, anonymisation and pseudonymisation, such tools being used only at the explicit request or approval of the data holder or data subject and third-party tools offered in that context not being used for other purposes".
[112] Art. 11, par. 7, Proposta di DGA.
[113] Art. 11, par. 8, Proposta di DGA.

di integrità e riservatezza e la disciplina inerente alla sicurezza del trattamento,[114] anche nei confronti delle informazioni di natura non personale.

Da ultimo, per quanto concerne il profilo procedurale, la disciplina non mostra particolare rigidità, in quanto l'imposizione di passaggi burocratici eccessivamente onerosi rischierebbe di compromettere la crescita florida e copiosa di questo nuovo attore del mercato dei dati.[115] L'articolo 10 stabilisce che l'attività di intermediazione può essere avviata in seguito all'invio di una notifica all'autorità che lo Stato membro designa come competente, senza che sia necessario attendere la concessione di autorizzazione alcuna.[116] A questo iter piuttosto snello fa da contraltare il potere di monitoraggio riconosciuto all'autorità pubblica, alla quale vengono conferiti poteri di controllo attraverso l'accesso alle informazioni, di richiamo e di richiesta di cessazione della violazione in caso di inottemperanza alle regole, fino alla possibilità di imporre sanzioni economiche o la cessazione del servizio.[117]

Siffatta caratterizzazione della figura dell'intermediario risponde all'esigenza di infondere fiducia nella condivisione dei dati in seno al mercato digitale europeo. La possibilità di fare affidamento su una figura intermedia a cui è vietato entrare in concorrenza con gli altri operatori potrebbe rivelarsi la chiave di volta per stimolare un flusso dei dati efficiente, caratterizzato da costi di transazione contenuti, elevata qualità dei dati e standard comuni. In altri termini, il tentativo del DGA è quello di promuovere lo sviluppo della *privacy by design* (del GDPR) in un contesto favorevole di *data by design*, in

[114] Art. 5, par. 1, lett. f) e art. 32, GDPR.
[115] *Workshop on labels for or certification of providers of technical solutions for data exchange*, *op. cit.*, p. 4.
[116] Art. 10, par. 4, Proposta di DGA.
[117] Art. 13, Proposta di DGA.

assenza del quale anche la protezione dei dati personali rischia di rimanere un astratto anelito normativo. Al contempo però, il requisito della neutralità può servire l'ulteriore scopo di impedire alle *big tech* di entrare in questo nuovo settore di mercato dove il vantaggio competitivo di cui già godono in virtù della loro posizione di privilegio causerebbe una illegittima alterazione della concorrenza. Come è stato osservato, la Proposta pone le condizioni per la creazione di una "nicchia di mercato" popolata da imprese europee,[118] specie piccole e medie, che sia indipendente da "qualsiasi operatore che detenga un grado significativo di potere di mercato".[119]

In sostanza, ad avviso della Commissione lo sviluppo dell'ecosistema digitale europeo passa anche attraverso la figura mancante dell'intermediario di dati. Se il *data sharing* rappresenta il mezzo che permetterà all'Unione europea di realizzare un modello differente, è possibile sostenere che l'intermediario, mentre "inventa" e determina l'infrastruttura di *governance* del digitale, ricoprirà il ruolo di pilota, poiché è su questi che grava il compito di separare chiaramente la messa a disposizione, l'intermediazione e l'utilizzo dei dati e di creare un ambiente aperto, equo e democratico che sia capace di accantonare, o almeno affiancare, il sistema delle grandi piattaforme.[120]

4. Spazio comune europeo di dati: *interdependence model versus independence model*

La commistione fra l'uniformità e l'immediata applicabilità della fonte regolamentare, da un lato, e le disposizioni che spesso

[118] IANNUZZI A., *La governance europea dei dati nella contesa per la sovranità digitale*, *op. cit.* pp. 42-44.
[119] Proposta di DGA, cons. n. 22.
[120] Proposta di DGA, cons. n. 25.

assumono le sembianze di uno strumento di incoraggiamento piuttosto che di carattere imperativo, dall'altro, rendono il DGA un provvedimento di stampo ibrido. La scelta di simile tecnica legislativa riflette la volontà del legislatore europeo di procedere con cautela e gradualità verso la realizzazione di uno spazio comune europeo di dati (*common European data space*), inteso quale "mercato unico dei dati nel quale questi ultimi possano essere utilizzati indipendentemente dal loro luogo fisico di conservazione nell'Unione, nel rispetto della normativa applicabile". Tuttavia, sono i sottospazi settoriali che lo compongono a costituire il vero "core tissue of an interconnected and competitive data economy in the EU".[121] Si tratta di ecosistemi di *governance* collettiva in cui la condivisione dei dati favorisce un ampliamento della gamma di utilizzatori pubblici e privati nel contesto dei settori aventi ad oggetto attività economiche, strategiche o di pubblico interesse per l'Unione.[122]

Il DGA mira per l'appunto a stabilire regole di principio comuni per tutti gli ambiti in cui la gestione dei dati ha un impiatto elevato sul sistema continentale, senza tuttavia soffocare la nascita di normative di settore specifiche – queste sì più rigorose – che tengano conto delle differenze che caratterizzano i singoli contesti produttivi.[123] Fondamentalmente, l'operatività degli spazi di dati passa attraverso un meccanismo di *governance* che traduca i principi europei in materia di trattamento e gestione dei dati in misure legislative, amministrative e contrattuali, idonee ad indirizzare lo

[121] Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal, *op. cit.*, p. 11.
[122] Proposta di DGA, cons. n. 2.
[123] Comunicazione della Commissione, "Una strategia europea per i dati", *op.cit.*, pp. 5-6. La Commissione distingue nove spazi specifici in ragione della loro particolare rilevanza per gli interessi europei: manifattura, *green deal*, mobilità, sanità, finanza, energia, agricoltura, pubblica amministrazione, competenze.

sviluppo di ambienti sicuri di condivisione e accesso ai dati senza che i confini digitali dei singoli Stati membri costituiscano un ostacolo.[124] Simile accorgimento risulta più che opportuno sia al fine di evitare la cosiddetta "data policy pitfall", ossia la convinzione che una normazione uniforme e sconnessa dal contesto sia in grado di trovare risposte adeguate ad una problematica pluridimensionale,[125] sia per l'incremento della qualità dei dati, piuttosto che della quantità, in quanto variabile che, al pari della natura del dato, risulta pesantemente influenzata da fattori contestuali e teleologici.[126] In questo senso, la Proposta di DGA, differentemente da quanto accade nella Proposta di Data Act, non offre rimedi di pronto utilizzo ma, proprio per mezzo dell'instaurazione degli spazi di dati, pone le basi per fornire soluzioni praticabili alle questioni evidenziate nel corso del presente lavoro.[127]

In primo luogo, il provvedimento si presta ad essere impiegato quale strumento di carattere "geopolitico" nella misura in cui la creazione di una zona continentale di gestione dei dati appare funzionale all'innalzamento una barriera virtuale di protezione da

[124] European Commission, Regulatory scrutiny board opinion, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), (SEC(2020) 405), p. 1.
A tale riguardo, malgrado non venga espressamente menzionata, il sistema di *data governance* in discussione sembra porsi in continuità con il progetto GAIA-X, ossia l'infrastruttura digitale di matrice europea proposta congiuntamente dai Ministeri dell'economia tedesco e francese. In proposito, si veda: *GAIA-X: A Pitch Towards Europe. Status Report on User Ecosystems and Requirements*, Federal Ministry for Economic Affairs and Energy (BMWi), 2020.
[125] OECD, *Enhancing Access to and Sharing of Data*, *op. cit.*, p. 78.
[126] L'Organizzazione per la cooperazione e lo sviluppo economico definisce la qualità dei dati in ambito statistico come un concetto poliedrico costituito da sette diverse dimensioni: *relevance, accuracy, credibility, timeliness, accessibility, interpretability, coherence, cost-efficiency*. Sul punto, si veda: OECD, *Quality framework and guidelines for OECD statistical activities*, version *2011/1 (STD/QFS(2011)1)*, pp. 7-11.
[127] Tuttavia, è bene sottolineare come la dottrina abbia criticato la penuria di disposizioni presenti nella Proposta di DGA atte a disciplinare la creazione degli spazi comuni di dati, atteso che, nella parte prescrittiva, vengono richiamati solamente in una occasione. Sul punto si veda: BALOUP J. ET AL., *White Paper on the Data Governance Act*, *op. cit*., p. 55.

ingerenze esterne indebite. Con questa iniziativa l'Unione vuole recuperare ad alcuni errori che essa stessa riconosce di aver commesso in passato, quando all'intenso utilizzo dei servizi digitali da parte dei cittadini europei non è corrisposto un adeguato sviluppo di piattaforme domestiche in grado di supportarli. Difatti, è proprio dal connubio di tali fattori che è scaturita l'invasione delle *big tech* statunitensi e cinesi e la conseguente dipendenza che gli Stati membri hanno sviluppato nei loro confronti.[128]

Orbene, se nella "battaglia" per la raccolta dei dati personali si è fatta trovare impreparata di fronte alle capacità delle compagini provenienti da Stati Uniti e Cina, ora l'Unione europea vuole affermarsi come *leader* sul nuovo versante degli "*industrial data*".[129] Il modello europeo di *governance* proposto con il DGA costituisce il provvedimento in cui le rivendicazioni eurounitarie si avvertono in maniera più compiuta.[130] Il raggiungimento di siffatta finalità passa necessariamente attraverso il contenimento della fuoriuscita dei dati dal territorio europeo, da un lato, e l'incremento della loro circolazione fra soggetti stabiliti all'interno dell'Unione, dall'altro. Pertanto, la via di uscita da tale congiuntura pregiudizievole per gli interessi europei prevede la creazione di un sistema infrastrutturale e regolamentare di matrice continentale su cui le imprese private e

[128] TOMBAL T., *Economic Dependence and Data Access*, in *International Review of Intellectual Property and Competition Law* (IIC), Issue 51 (1), 2020, pp. 70 e ss.

[129] Eloquenti le parole del Commissario europeo per il mercato interno e i servizi Thierry Breton il quale in un intervento del 15 febbraio 2020 ha affermato: "Europe may have lost the battle to create digital champions capable of taking on U.S. and Chinese companies harvesting personal data, but it can win the war of industrial data" e ancora "We're entering a new phase. The battle for industrial data starts now, and the main battlefield will be Europe". Le parole sono prese da ROSE M., *Europe can win global battle for industrial data, EU industry chief says*, Reuters, 15-02-2020, disponibile al link: https://www.reuters.com/article/eu-data-idUSL8N2AF0FO.

[130] IANNUZZI A., *La governance europea dei dati nella contesa per la sovranità digitale*, *op. cit.* pp. 48-52.

gli enti pubblici possano fare affidamento per la gestione delle informazioni in loro possesso.

A tale proposito, il modello europeo di *data governance* racchiude il potenziale per una indispensabile riconsiderazione della anacronistica impostazione della normativa europea, al fine di includere concetti quali la dipendenza della qualificazione del dato dal contesto operativo e l'approccio basato sul rischio per la gestione di tutti i tipi di dati. L'accesso ai dati e la natura degli stessi sono fattori strettamente correlati: il carattere personale implica, di regola, un regime di accesso più restrittivo rispetto ad informazioni non personali che, al contrario, potranno godere di maggiore pubblicità. La stessa interdipendenza non può che riguardare anche il rischio di gestione che, al pari del dato, è *context-dependent*.[131] Dunque, il modello di *governance* potrebbe condurre verso la creazione di un ecosistema più sicuro nel cui ambito si affronta e si gestisce un rischio ineludibile, nella misura in cui consentirà una costante e progressiva valutazione dei pericoli sottesi al trattamento dei dati non solo nel contesto del titolare originario, ma anche nell'insieme delle operazioni di trasferimento precedenti e successive.[132] L'avvicinamento alla prospettiva contestuale presente nel DGA si percepisce in misura significativa dal considerando n. 15 della versione recentemente approvata dal Parlamento,[133] nella parte in cui,

[131] MANTELERO A., *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le Nuove Leggi Civili Commentate*, n. 1/2017, pp. 144 ss.
[132] CAVOUKIAN A., CASTRO D., *Big Data and Innovation, Setting the Record Straight: De- identification Does Work*, 2014, *op. cit.*, pp. 9-11.
[133] La parte del considerando in commento che assume qui rilievo recita: "Qualora la fornitura di dati anonimizzati o modificati non rispondesse alle esigenze del riutilizzatore, a condizione che siano stati soddisfatti i requisiti di svolgere una valutazione d'impatto in materia di protezione dei dati e consultare l'autorità di controllo ai sensi degli articoli 35 e 36 del regolamento (UE) 2016/679 e qualora i rischi per i diritti e gli interessi degli interessati risultino minimi, potrebbe essere consentito il riutilizzo in loco o remoto dei dati in un ambiente di trattamento sicuro. Ciò potrebbe costituire una soluzione adeguata per il riutilizzo dei dati pseudonimizzati. È opportuno che le analisi dei dati in tali ambienti di

introducendo il concetto di "ambiente di trattamento sicuro", sembra dare maggiore risalto ai fini del corretto bilanciamento tra protezione dei dati e libera circolazione, al "chi" (titolare dei dati) e al "come" (modalità di gestione dei dati), piuttosto che al "cosa" (il dato in sé). Sebbene non sia presente uno stravolgimento della concezione della natura delle informazioni – viene specificato, ad esempio, che i dati pseudonimizzati "mantengono il loro status di dati personali" – per una volta il discrimine non sembra basarsi solamente sulla qualifica giuridica del dato, ma anche sul regime metodologico di trattamento degli stessi e sulla conseguente capacità di minimizzare i rischi per i diritti e gli interessi dei soggetti coinvolti. In questo sostanzialmente è percepibile un passo in avanti decisivo da parte del legislatore europeo rispetto al paradigma precedente.

Inoltre, ora l'applicazione di siffatte tecniche volte a ridurre l'identificabilità o la rivelazione delle informazioni si inserisce in appositi spazi di dati dove possono trovare posto, al fianco degli strumenti di carattere matematico-scientifico già in uso, misure che attribuiscono il giusto peso anche agli altri fattori, specie umani, che possono avere un impatto sulla tutela dei dati.[134] Con la prospettiva della promulgazione di discipline settoriali, appare decisamente più vicino l'obiettivo della standardizzazione di procedure di anonimizzazione calibrate sui rischi tipici di ognuno dei *data spaces*; elemento fondamentale per infondere maggior chiarezza con

trattamento sicuri siano controllate dall'ente pubblico al fine di proteggere i diritti e gli interessi di terzi. In particolare, i dati personali dovrebbero essere trasmessi a terzi per il riutilizzo soltanto laddove una base giuridica conforme alla legislazione sulla protezione dei dati consenta tale trasmissione. I dati non personali dovrebbero essere trasmessi solo quando non vi è motivo di ritenere che la combinazione di set di dati non personali condurrebbe all'identificazione degli interessati. Ciò dovrebbe valere anche per i dati pseudonimizzati che mantengono il loro status di dati personali".

[134] OHM P., *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, UCLA Law Review, Vol. 57, 2010, pp. 1706.

riguardo alle operazioni di qualificazione della natura dei dati.[135] Un ambiente dove è stabilito a monte quali tecniche devono essere applicate per rendere i dati anonimi risulta particolarmente fertile per l'introduzione di apposite *fictio iuris* o presunzioni legali al ricorrere delle quali il dato può essere considerato non personale nella misura in cui è stato anonimizzato secondo quanto previsto dalla disciplina dello specifico spazio di dati di interesse.[136] Il fatto che tale soluzione possa anche tradursi in un ostacolo alla circolazione delle informazioni tra i diversi spazi, in quanto rispondenti a regole differenti, non rappresenta necessariamente un difetto del sistema. Al contrario, si impedirebbe che l'impiego di *dataset* generati in seno ad un determinato ambiente producano risultati inesatti e persino deleteri quando vengono utilizzati come risorsa in ambiti totalmente differenti.[137] In un certo senso, la regolazione settoriale dell'anonimizzazione appare l'unico modo per continuare ad utilizzare dati non personali garantendo il rispetto degli obblighi, *ex lege* o contrattuali, di non re-identificazione e senza sacrificare totalmente la loro utilità.

D'altro canto, i *data spaces* potrebbero rivelarsi una soluzione ottimale anche con riguardo alle questioni riguardanti la *data ownership*, e, pertanto, potrebbero costituire il mezzo ideale per garantire un'effettiva attuazione delle disposizioni in materia di accesso contenute nelle Proposta di Data Act. L'ubiquità dei dati e le

[135] AGCM, AGCOM, Garante per la protezione dei dati personali, *Indagine conoscitiva sui big data*, 2018, p. 23-25.
[136] L'idea di introdurre delle presunzioni in materia di anonimizzazione deriva dal lavoro del gruppo denominato *Data Ethics Commission* (*Datenethikkommission*), costituito da esponenti provenienti dai settori accademico, amministrativo e industriale, istituito dal governo tedesco nel 2018 allo scopo di elaborare alcune proposte in riferimento ai principali quesiti etico-giuridici afferenti ai sistemi algoritmici e ai dati. In proposito, si veda: *Opinion of the Data Ethics Commission*, 2019.
[137] DE LAAT P., *Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?*, in *Philos. Technol*. 31, 2018, pp. 525-541.

relative problematiche in punto di diritto sono fortemente amplificate nei settori indicati come strategici per il mercato europeo, specie nella *smart manufacturing*, in cui l'informazione non rappresenta il frutto di operazioni realizzate da un unico soggetto, ma, viceversa, di più operatori.[138] Il contributo che ognuno di essi ha apportato alla generazione del dato e la conseguente corretta allocazione dei relativi diritti potranno trovare migliore sistematizzazione in seno ad ambienti sicuri, dove anche i compiti di supervisione affidati alle autorità di controllo potranno essere svolti con incisività ed efficacia.[139]

In aggiunta, nello scenario in esame risulta apprezzabile la scelta di affidare agli intermediari di dati il ruolo cardine del sistema europeo. La predisposizione di un "filtro" nell'ambito dei flussi di informazioni consentirebbe di superare alcuni fra i più spinosi problemi caratterizzanti l'analisi e il riutilizzo dei dati. Tra l'altro, la strutturazione dei servizi di intermediazione prospettata nel DGA si rivela estremamente preziosa per quella consistente porzione del mercato continentale costituita da piccole e medie imprese, le quali si trovano costantemente costrette a fronteggiare serie difficoltà con riguardo alla corretta identificazione dei dati che possono essere condivisi o riutilizzati senza infrangere norme di legge o accordi privati.[140] In tal senso, l'intermediazione rappresenta il vero motore per aumentare la fiducia nei confronti della condivisione, promuovere standard specifici per ogni settore a beneficio dell'interoperabilità e, infine, procedere ad una maggiore distribuzione del potere di mercato.

---

[138] WIEBE A., *Protection of industrial data – a new property right for the digital economy?*, in *Journal of Intellectual Property Law & Practice*, 2016.
[139] Capo IX, Proposta di Data Act.
[140] Commission Staff Working Document, *Guidance on sharing private sector data in the European data economy*, *op. cit.*, p. 1.

Il carattere innovatore della Proposta di DGA risiede altresì nella scelta di adottare un corpo di regole di principio dove viene lasciato spazio ad interventi dal basso. In tal guisa, il legislatore manifesta il desiderio di allontanamento sia dal sistema statunitense che da quello cinese, i quali rappresentano, nell'attuale contesto di *data dependence*, sfumature differenti di quello che potremmo definire "*independence model*", dove il trattamento e la gestione dei dati risponde ad una logica verticale e centralizzata, caratterizzata da un elevato grado di indipendenza – del soggetto privato o di quello pubblico – nei confronti dei concorrenti. A tale riguardo, infatti, è possibile distinguere, da un lato, la versione statunitense orientata ad un approccio di autoregolamentazione pura che conduce al consolidamento di posizioni di dominio da parte dei soggetti che offrono servizi OTT,[141] mentre dall'altro lato, il paradigma cinese che si caratterizza per un pesante controllo statale sulle iniziative private nell'intento di assicurare al soggetto pubblico l'accesso ad una quantità di dati più vasta.[142]

Per converso, nessuna delle due varianti dell'*independence model* sarebbe riproducibile in territorio europeo, se non sacrificando i valori fondamentali su cui poggia la disciplina continentale in materia di trattamento dei dati. Il modello americano non risulta replicabile per ragioni logiche e pratiche, ancor prima che giuridiche, giacché non esiste, allo stato, un'impresa europea operante nel settore della gestione dei dati in grado di assicurare prestazioni equiparabili a quelle degli omologhi con sede oltreoceano. Al contempo, anche il modello asiatico non pare possa trovare

[141] Ferma restando l'accessibilità garantita ai dati detenuti da tali soggetti da parte del governo statunitense per mezzo del Clarifying Lawful Overseas Use of Data Act (Cloud Act). Per un approfondimento in merito, si veda: BONCINELLI V., *Modelli tecnici e disciplina giuridica del c.d. cloud computing*, *op. cit.*, pp. 34-38.
[142] Comunicazione della Commissione, "Una strategia europea per i dati", *op.cit.*, p. 4.

affermazione in Europa, in quanto rispondente ad una logica prettamente autoritaria che non collima con i principi costituzionali da cui mutua l'ordinamento europeo, specie in materia di trattamento dei dati personali. Pertanto, nel tentativo di percorrere una strada propria, il DGA promuove un sistema qualificabile come "*interdependence model*", ispirato ad un'ottica collaborativa secondo cui differenti soggetti sono chiamati a (co)operare sulla base di una relazione di stretta interdipendenza, funzionale sia alla circolazione dei dati che alla distribuzione del potere di mercato. In tal senso, attraverso la disciplina di un'infrastruttura concepita come neutrale e aperta, il legislatore non persegue l'obiettivo dell'esclusione altrui come accade nell'*independence model*, ma favorisce l'instaurazione di rapporti di interdipendenza tra operatori, anche provenienti dall'esterno, i quali sono chiamati ad agire nel rispetto delle regole del sistema.

In conclusione di questa disamina, è possibile sostenere che tanto il DGA quanto il Data Act contengono indizi utili al fine di qualificare il *data law* europeo. L'approccio che pervade le proposte in esame è caratterizzato da elementi parzialmente differenti rispetto al passato. Sebbene alcuni timori fossero già presenti con riguardo alle informazioni non personali,[143] in questi provvedimenti si avverte in maniera più decisa la tendenza alla "mercificazione" del dato, il quale, pertanto, diventa l'oggetto diretto della regolazione. Questo aspetto assume particolare rilievo se si considera che il DGA disciplinerà anche la *governance* dei dati personali: non viene plasmata una disciplina destinata a proteggere le persone fisiche

[143] Parere del Comitato economico e sociale europeo (CESE) sulla "Comunicazione della Commissione al Parlamento europeo e al Consiglio - Linee guida sul regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea" adottato il 25 settembre 2019.

nell'ambito del trattamento delle informazioni che le riguardano, ma viene regolata la gestione di tali informazioni in qualità di asset autonomo e slegato dall'entità cui inerisce.[144] Sebbene queste ultime proposte possiedano il potenziale per avviare una transizione in tal senso, il percorso che il diritto dei dati europeo si accinge ad intraprendere si rivelerà certamente lungo e tortuoso, principalmente in ragione dell'insistenza di parte delle istituzioni unionali nel rivendicare la dogmatica "superiorità" normativa del GDPR, che, se non opportunamente declinata nel contesto della *data governance*, rischia di rimanere lettera morta.

La scissione tra dato ed entità che esso descrive non può che generare profonde ripercussioni anche con riguardo ai profili definitori della fattispecie. Malgrado, le definizioni originarie di dati personali e non personali vengano riprese testualmente, la vena che percorre le Proposte sembra dirigersi verso una maggiore uniformazione delle due categorie su cui oggi è costruito il diritto europeo in materia di dati. A conferma di ciò, anche il Comitato europeo per la protezione dei dati e il Garante europeo della protezione dei dati si accorgono di questa tendenza e, nei passaggi più critici del loro parere congiunto, intervengono rimarcando la profonda differenza che intercorre fra i dati personali e quelli non personali, chiedendo che tale separazione non venga intaccata dal nuovo provvedimento.[145] Malgrado ciò, le crescenti difficoltà di distinzione tra differenti classi di dati e, soprattutto, gli altrettanto gravi pericoli che possono derivare dal trattamento di quelli non personali, lasciano scorgere un incipiente spostamento dalla originaria disciplina delle singole categorie di dati ad un diritto dei dati unitario ed onnicomprensivo, una "regolazione orientata a

[144] BALOUP J. ET AL., *White Paper on the Data Governance Act*, *op. cit.*, pp. 54-55.
[145] EDPB-GEPD, Parere congiunto 03/2021, *op. cit.*

proteggere i dati da un punto di vista generale",[146] dove la nozione di dato personale come la conosciamo oggi rischia di essere messa definitivamente da parte.[147]

[146] AGCM, AGCOM, Garante per la protezione dei dati personali, *Indagine conoscitiva sui big data*, *op. cit*., p. 45.
[147] PURTOVA N., *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, in *Law, Innovation and Technology*, Vol. 10, No. 1, 2018, pp. 78-80.

CONCLUSIONI

Il presente lavoro di tesi è stato sviluppato con l'intento di fornire una possibile risposta agli interrogativi riguardanti la solidità e l'adeguatezza del diritto europeo dei dati in un'epoca – quella attuale – caratterizzata da cambiamenti tecnologici rivoluzionari.[1] La domanda assume particolare rilevanza alla luce delle sfide che le stesse istituzioni continentali, specie con l'elaborazione delle "Strategia europea per i dati", hanno indicato come fondamentali, in quanto dalla corretta implementazione delle relative soluzioni dipende la sopravvivenza dell'Unione europea come organizzazione internazionale e degli Stati membri, i quali individualmente non possono nemmeno sperare di reggere il confronto con Stati Uniti d'America e Repubblica Popolare Cinese.

Per adempiere ai propositi fissati nella parte introduttiva, la tesi ha, in primo luogo, ripercorso le tappe salienti che hanno condotto l'ordinamento europeo verso il consolidamento di una disciplina puntuale e fortemente protettiva con riguardo ai dati personali, in ragione della costituzionalizzazione del diritto alla tutela di tale tipologia di informazioni. L'indagine dell'evoluzione ordinamentale ha avuto il pregio di evidenziare la pertinenza e la congruità dell'operato dei legislatori dei Paesi membri e della (futura) Unione europea, atteso che la conformazione del quadro giuridico illustrato è perfettamente in linea con i valori sviluppatisi nei sistemi normativi continentali nel corso del secondo dopoguerra.[2] Al contempo, la prospettiva storica ha consentito una adeguata comprensione dei motivi che hanno determinato la delimitazione dei

[1] SIMONCINI A., *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 2019, 63 ss.
[2] *Supra* cap. I, par. 2.

rispettivi ambiti di applicazione delle discipline relative alle due categorie di informazioni prese in esame e il pronunciato divario che ne è conseguito.

Il Regolamento (UE) 2018/1807, oltre a non attribuire alcun diritto sostanziale significativo a chi gode della disponibilità di dati non personali, prescrive una gamma di regole in materia di circolazione dalla quale è possibile apprezzare compiutamente l'esiguità del peso specifico che il legislatore ha riservato alla categoria delle informazioni non personali rispetto a quelle personali. Le condizioni che assoggettano il trasferimento dei dati personali al di fuori dell'Unione si traducono in una misura di *data localization* che, al contrario, non è rinvenibile nel regime di circolazione extraeuropea delle informazioni non personali. [3] Per converso, l'incremento esponenziale dei dati non personali causato dal fenomeno della datificazione ha sollevato nuove perplessità in merito alla attitudine di tali regole a governare il sistema di gestione dei dati nella maniera più proficua e costruttiva per gli interessi dell'Europa e degli Stati Membri.

La tesi della fragilità della struttura dell'impianto normativo attualmente vigente sostenuta nell'ambito del presente lavoro cerca conferme tramite l'esame delle questioni che attengono alla corretta qualificazione giuridica dei dati. L'esplorazione delle prescrizioni che regolano l'identificazione della natura delle informazioni trattate restituisce uno spaccato chiaro delle difficoltà cui vanno incontro tanto i soggetti che gestiscono grandi moli di dati, specie se insiemi misti, quanto gli stessi interpreti che si trovano costretti a ricorrere a categorie che fenomeni come *Big Data* e *data analysis* hanno ormai condannato all'obsolescenza.

[3] *Supra* cap. II.

A tale riguardo, la classe di dati che forse più di altre dà prova dell'attrito esistente tra natura giuridica delle informazioni e progresso tecnologico è quella dei dati anonimizzati: se, da un lato, l'irreversibilità della re-identificazione costituisce ancora lo standard di riferimento secondo l'interpretazione fornita dal Gruppo di lavoro articolo 29, dall'altro lato, gli esperti sono ormai concordi nell'affermare che nessun dato anonimizzato, se vuole mantenere anche un minimo coefficiente di utilità, può considerarsi esente dal rischio di re-identificazione. Dalla constatazione di siffatto contrasto nascono le istanze mostrate in più di un'occasione dalla dottrina che da tempo invita il legislatore a rivedere le regole in tema di procedure di anonimizzazione.[4]

Sul versante della circolazione, invece, sono le questioni relative alla proprietà dei dati a ricoprire un ruolo centrale. Sebbene le prime valutazioni in merito abbiano attirato le attenzioni della dottrina di stampo economico, è evidente che l'allocazione di una risorsa così preziosa per le industrie e per le pubbliche amministrazioni rappresenta un argomento che non può rimanere al di fuori del dibattito giuridico, specialmente quello costituzionale. Garantire o escludere l'accesso alle informazioni raccolte o comunque generate nel contesto dell'utilizzo di macchinari intelligenti si traduce in una scelta politico-giuridica con ripercussioni radicali e diffuse. Assumendo ancora una volta la prospettiva degli operatori della manifattura intelligente, la questione della proprietà si tramuta in questione di sopravvivenza, quantomeno per quelle piccole e medie imprese che popolano il territorio italiano ed europeo, le quali, nell'ipotesi in cui venissero tagliate fuori dalla possibilità di accedere alle informazioni raccolte

[4] *Supra* cap. III, par. 3.1.

dagli strumenti impiegati nella fase di produzione, non avrebbero più il potere di innovare i propri processi e i propri modelli e, dunque, perderebbero la capacità di essere competitive. In tale ipotesi, l'appello rivolto dalla dottrina al legislatore affinché chiarisca in via di diritto una situazione di fatto che rimane, in gran parte, non presidiata da alcuna regola, appare tutt'altro che omogeneo. Al riguardo, la disamina della dottrina rilevante ha, però, dimostrato che la maggioranza delle voci propende per una politica di incentivazione dei diritti di accesso ai dati in favore di tutti quei soggetti che, tramite le loro azioni, hanno contribuito alla generazione di tali informazioni, opponendosi in tal modo alle teorie dei fautori dell'introduzione di una vera e propria privativa.[5]

Dopo la ricognizione *de iure condito*, la parte finale della tesi si proietta in avanti alla ricerca di elementi che possano indicare quali mutamenti interesseranno il diritto europeo dei dati nel prossimo futuro. Con le proposte più recenti, sembra che l'Unione europea abbia constatato l'esistenza di alcune falle nell'ordinamento e che si stia muovendo per fornire una possibile risposta. In tal senso, i documenti presi in considerazione, pubblicati nel corso dello svolgimento della ricerca, hanno in parte avvalorato quanto sostenuto nei capitoli precedenti.

A tale proposito, risulta di primario interesse il modello "europeo" di *governance* dei dati, il quale altro non è che lo strumento attraverso cui le istituzioni continentali hanno deciso di affrontare gli ostacoli creati dall'accumulo di potere in capo a quei soggetti, pubblici e privati, esterni al circuito dell'Unione. La Commissione europea non fa mistero della volontà di realizzare un sistema che la metta al riparo dalle insidie alla sua sovranità

[5] *Supra* cap. III, par. 3.2.

provenienti da Paesi terzi, su tutti Stati Uniti e Cina, e a tale scopo ipotizza la realizzazione di un apparato nuovo, differente dalle realtà di gestione dei dati attualmente dominanti. La finalità di tale modello non risiede solamente nel desiderio di contribuire ad una distribuzione equanime delle risorse per mezzo del *data sharing*, ma altresì nella volontà di impedire che i dati generati in territorio continentale possano divenire una risorsa per una autorità o un'industria extraeuropea.[6]

Per tali ragioni, è possibile sostenere che anche l'Unione europea si sia inserita sulla scia del fenomeno definito come "*Data Nationalism*",[7] sintagma utilizzato per descrivere la pratica frequente nelle normative di *data law* di conformarsi a politiche di localizzazione dei dati come reazione ad iniziative ostili provenienti dall'esterno.[8] Siffatta tendenza viene corroborata dalle disposizioni in tema di trasferimento all'estero dei dati non personali che trovano ora dimora – salve eventuali modifiche prima dell'approvazione definitiva – sia nel Data Governance Act che nel Data Act; mentre, verosimilmente, la collocazione più opportuna sarebbe stata all'interno della fonte avente come oggetto specifico la circolazione delle informazioni non personali, dunque il Regolamento (UE) 2018/1807. Questa "correzione" che il legislatore intende apportare al diritto dei dati sembra indicare che il nuovo ordinamento si stia muovendo verso un rinnovato bilanciamento tra dati personali e dati non personali, vuoi perché sta diventando sempre più complicato

[6] *Supra* cap. IV, par. 2.
[7] L'espressione in parola è riconducibile a: CHANDER A., LÊ U. P., *Data Nationalism*, in *Emory Law Journal*, Vol. 64, Iss. 3, 2015.
[8] DELLA MORTE G., *Big Data e Protezione Internazionale Dei Diritti Umani. Regole e Conflitti*, in ARCARI M., MILANO E., TANZI. A. (diretta da), *La ricerca del diritto nella comunità internazionale*, Editoriale scientifica, Napoli, 2018, p. 279.

distinguere gli uni dagli altri, vuoi perché i secondi stanno acquisendo maggiore importanza.[9]

Scendendo nel dettaglio, malgrado le proposte non si spingano sino ai lidi della regolazione dell'anonimizzazione, il modello di *governance* proposto racchiude tutte le potenzialità per divenire terreno fertile per lo sviluppo di un rinnovato approccio al tema. Nello specifico, particolarmente promettente potrebbe rivelarsi la figura dell'intermediario di dati, il quale, grazie al carattere neutrale della sua funzione, costituisce il soggetto migliore per ricoprire la posizione di "filtro" tra coloro che trattano dati personali e chi, dall'altro lato, desidera accedere a informazioni utili per la propria attività, senza per questo assumere la qualifica di titolare del trattamento ai sensi del GDPR. Le ultime modifiche apportate alla proposta originaria di DGA, che in prima battuta non prevedeva per l'intermediario la facoltà di anonimizzare, lasciano ben sperare per il futuro sviluppo dei servizi di intermediazione come motore per un'analisi dei dati funzionale e rispettosa degli interessi individuali.[10]

Infine, la proposta di Data Act sembra destinata a incidere significativamente sul tema della proprietà dei dati in territorio europeo. La versione del documento pubblicata a febbraio 2022 sembra scongiurare l'introduzione di una privativa in favore di uno solamente fra i soggetti che hanno contribuito alla generazione del dato, per aderire, invece, alla alternativa dell'accesso. Ancora una volta, traspare la volontà di schierarsi dalla parte del soggetto più debole del rapporto – l'utente o il terzo desideroso di avere accesso ai dati – per compensare lo squilibrio rispetto alle grandi compagnie che, solitamente, hanno la capacità tecnica di escludere gli altri dalla

[9] *Supra* cap. IV, par. 3.1.
[10] *Supra* cap. IV, par. 3.2.2.

disponibilità dei dati. In questo come negli altri casi, lo scopo dell'Unione rimane pur sempre quello di riconquistare il terreno sovrano perduto perché, nel rapporto di forza con le altre potenze tecnologiche, è l'organizzazione continentale a ricoprire la posizione di soggetto debole.

In conclusione, è possibile affermare che il diritto europeo dei dati sia in procinto di attraversare una fase di ulteriore cambiamento, consapevole del fatto che per affrontare con successo sfide nuove non è possibile fare ricorso – solamente – a categorie interpretative appartenenti al passato, giacché si rivela di vitale importanza elaborare strumenti originali *ad hoc*.[11] In questo senso, se la regolazione della tecnologia richiede l'integrazione di norme di estrazione differente, la creazione dello "spazio comune europeo di dati" potrebbe presto divenire quell'ambiente dove norme di carattere giuridico, economico e tecnico si confrontano alla costante ricerca di un dinamico equilibrio.[12]

[11] RODOTÀ S., *Il mondo nella rete – Quali diritti, quali vincoli*, Laterza, Bari, 2014, p. 67.
[12] OHM P., *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, UCLA Law Review, Vol. 57, 2010.

BIBLIOGRAFIA

Dottrina

ABRAHAMSON Z., *Essential Data,* in *Yale Law Journal*, vol. 124, no. 3, 2014

ABRAMS M., *The Origins of Personal Data and its Implications for Governance,* The Information Accountability Foundation, 2014

ADAM R., *Da Colonia a Nizza: la Carta dei diritti fondamentali dell'Unione europea*, in *Il Diritto dell'Unione Europea*, n. 4/2000

AIELLO G. F., *La protezione dei dati personali dopo il Trattato di Lisbona, in Oss. del dir. civ. e comm., n. 2/2015*

ALLEGRI M. R., *Diritto all'oblio, tutela della web reputation individuale e "eccezione giornalistica": spunti giurisprudenziali*, in *Forum di Quaderni Costituzionali*, 2018

ALLEGRI M. R., *Ubi Social, Ibi Ius. Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei provider*, Milano, Franco Angeli, 2018

BALOUP J., EMRE BAYAMLIOĞLU, BENMAYOR A., DUCUING C., DUTKIEWICZ L., LALOVA T., MIADZVETSKAYA Y., PEETERS B., *White Paper on the Data Governance Act*, in *CiTiP Working Paper, KU Leuven Centre for IT & IP Law*, 2021

BAMBERGER K. A., LOBEL O., *Platform Market Power*, in *Berkeley Technology Law*, Journal 32, no. 3, 2017

BAUER M., FERRACANE M. F., LEE-MAKIYAMA H., VAN DER MAREL E., *Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States*, ECIPE Occasional Paper No. 3/2016

BAUER M., LEE-MAKIYAMA H., VAN DER MAREL E., VERSCHELDE B., *The Cost of Data Localisation: Friendly Fire on Economic Recovery*, ECIPE Occasional Paper No. 3/2014

BERNAL P., *Internet Privacy Rights. Rights to Protect Autonomy*, in *Cambridge Intellectual Property and Information Law*, *Cambridge University Press*, 2014

BIFULCO R., CARTABIA M., CELOTTO A., *Introduzione*, in BIFULCO R., CARTABIA M., CELOTTO A., L'Europa dei diritti, Bologna, 2001

BOMPREZZI C., *Implications of Blockchain-Based Smart Contracts on Contract Law*, *Luxembourg Legal Studies*, Vol. 23, Nomos, 2021

BONCINELLI V., *Modelli tecnici e disciplina giuridica del c.d. cloud computing*, in *Rivista italiana di informatica e diritto*, fasc. n. 1/2021

BRKAN M., BONNET G., *Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes*

and Fata Morganas, in *European Journal of Risk Regulation*, Vol. 11, Issue 1, 2020

BRUGIOTTI E., *La privacy attraverso le "generazioni dei diritti". Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico*, in *dirittifondamentali.it*, 2/2013

BYGRAVE L., *Information Concepts in Law: Generic Dreams and Definitional Daylight*, in *Oxford Journal of Legal Studies*, Vol. 35, No. 1, 2015

CAGGIANO G., *La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali*, in *Studi sull'integrazione europea*, 2018

CALIFANO L., *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, 2016

CALOPRISCO F., *Data Governance Act. Condivisione e "altruismo" dei dati*, in *Associazione Italiana Studiosi di Diritto dell'Unione europea* (AISDUE), *Focus "Servizi e piattaforme digitali"*, n. 3, 2021

CALZOLAIO S., *Gli ISP si salvano nel P2P. Ma reggeranno allo streaming?*, in *Forum di Quaderni costituzionali*, 2012

CALZOLAIO S., *Introduzione. Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati*, in *Rivista italiana di informatica e diritto*, fasc. n. 1/2021

CALZOLAIO S., *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in *federalismi.it*, n. 24/2017

CALZOLAIO S., *Protezione dei dati personali*, in BIFULCO R., CELOTTO A., OLIVETTI M., (a cura di), *Digesto delle Discipline Pubblicistiche*, Utet giuridica, 2017

CALZOLAIO S., *Sistema di allerta Covid-19. Osservazioni sull'art. 6, d.l. 28/2020*, in CALZOLAIO E., MECCARELLI M., POLLASTRELLI S. (a cura di), *Il diritto nella pandemia. Temi, problemi, domande*, 2020

CANTEKIN K., *Comity upon request. What does the new U.S. CLOUD Act tell us about the future of data flow regulation?*, in *Eurojus, Big data and Public Law: new challenges beyond data protection*, Numero speciale, 2018

CATE F. H., KUNER C., MILLARD C., SVANTESSON D. J., *Systematic Government Access to Private-Sector Data Redux,* in *International Data Privacy Law*, vol. 4, 2014

CAVOUKIAN A., *7 foundational principles of privacy by design*, Office of the Information & Privacy Commissioner of Ontario, 2010

CAVOUKIAN A., CASTRO D., *Big Data and Innovation, Setting the Record Straight: De- identification Does Work*, 2014

CHANDER A., LÊ U. P., *Breaking the Web: Data Localization vs. the Global Internet*, Working Paper 2014-1, in *California International Law Center*, 2014

CHANDER A., LÊ U. P., *Data Nationalism*, in *Emory Law Journal*, Vol. 64, Iss. 3, 2015

CHRISTAKIS T., TERPAN F., *EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options*, in *International Data Privacy Law*, Vol. 11, No. 2, 2021

COLPAERT C., JANSSENS M-C., *Work in progress: the proposal of the free flow of non-personal data regulation*, in *CITIP Blog*, 2018

COLAPIETRO C., IANNUZZI A., *App di contact tracing e trattamento dei dati con algoritmi: la falsa alternativa tra tutela del diritto alla salute e protezione dei dati personali*, in *Dirittifondamentali.it*, n. 2/2020

COLAPIETRO C., *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *federalismi.it*, n. 2/2018

COLAPIETRO C., *Tutela della dignità e della riservatezza del lavoratore nell'uso delle tecnologie digitali per finalità di lavoro*, in *Giornale di diritto del lavoro e di relazioni industriali*, Franco Angeli, Milano, 2017

CONTALDI G., *Il DMA (Digital Markets Act) tra tutela della concorrenza e protezione dei dati personali*, in *Ordine internazionale e diritti umani*, n. 2/2021

CONTALDI G., *Intelligenza artificiale e dati personali*, in *Ordine internazionale e diritti umani*, n. 5/2021

CORTESE B., *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Il Diritto dell'Unione europea*, n. 2 del 2013

D'ACQUISTO G., *Qualità dei dati e Intelligenza Artificiale: intelligenza dai dati e intelligenza dei dati*, in PIZZETTI F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, 2018

D'ACQUISTO G., NALDI M., *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, in *I diritti della "rete" nella rete*, Giappichelli, 2017

DALLA CORTE L., *Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protecton Law*, in *European Journal of Law and Technology*, Vol. 10, No. 1, 2019

DAVISON M. J., HUGENHOLTZ, P. B., *Football fixtures, horseraces and spin offs: the ECJ domesticates the database right*, in *European Intellectual Property Review*, n. 3, 2005

DE HERT P., GUTWIRTH S., *Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action,* in GUTWIRTH S.; POULLET Y.; DE HERT P.; NOUWT J.; DE TERWANGNE C. (eds), *Reinventing data protection?, ,* Springer, 2009

DE HERT P., PAPAKONSTANTINOU V., *The data protection regime in China, In-depth Analysis for the LIBE Committee*, 2015

DE LAAT P., *Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?*, in *Philos. Technol*. 31, 2018

DELLA MORTE G., *Big Data e Protezione Internazionale Dei Diritti Umani. Regole e Conflitti*, in ARCARI M., MILANO E., TANZI. A. (diretta da), *La ricerca del diritto nella comunità internazionale*, Editoriale scientifica, Napoli, 2018

DI GIOVANNI A., *I servizi di interesse generale tra poteri di autorganizzazione e concessione di servizi*, in *Nuovi problemi di amministrazione pubblica*, 2018

DREXL J., *Data Ownership and Access to Data. Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate* (documento redatto da DREXL J., HILTY R. M., DESAUNETTES L., GREINER F., KIM D., RICHTER H., SURBLYTĖ G., WIEDEMANN K.) 2016

DREXL J., *Designing Competitive Markets for Industrial Data – Between Propertisation and Access*, Max Planck Institute for Innovation & Competition Research Paper No. 16-13, 2016

DREXL J., *Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy*, Max Planck Institute for Innovation and Competition Research Paper No. 18-23, 2018

DUCATO R., *La crisi della definizione di dato personale nell'era del web 3.0. Una lettura civilistica in chiave comparata*, in CORTESE F., TOMASI

M. (a cura di), *Le definizioni nel diritto. Atti delle giornate di studio 30-31 ottobre 2015*, 2016

ELLIOT M., MACKEY E., *The Social Data Environment*, in O'HARA K., DAVID S. L., DE ROURE D., NGUYEN C. M-H. (eds.), *Digital Enlightenment Yearbook*, 2014

ELLIOT M., MACKEY E., O'HARA K., TUDOR C., *The anonymisation decision-making framework*, *Ukan Publications*, 2016

FARO S., *Trattamento dei dati personali e tutela della persona*, in *Digesto delle Discipline* Pubblicistiche, appendice di aggiornamento, Torino, Utet, 2000

FERRACANE M. F., *Restrictions on Cross-Border data flows: a taxonomy*, ECIPE Working Paper No. 1/2017

FIA T., *La tutela dei dati non personali: accesso, proprietà e regolamentazione*, in *Nuovo Notiziario Giuridico*, 2019

FINCK M., PALLAS F., *They who must not be identified – distinguishing personal from non-personal data under the GDPR*, in *International Data Privacy Law*, 2020, Vol. 10, No. 1

FINOCCHIARO G., *Identità personale (diritto alla)*, in *Digesto delle discipline privatistiche, Sezione civile*, Torino, 2010

FINOCCHIARO G., *Il diritto all'oblio nel quadro dei diritti della personalità*, in RESTA G., ZENO-ZENCOVICH V., (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Collana "Consumatori e Mercato", 2015

FINOCCHIARO G., *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a* Schrems, in RESTA, ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Collana "Consumatori e Mercato", 2016

FIORILLO V., *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di Giustizia dell'Unione europea*, in *federalismi.it*, n. 15/2017

FOCARELLI C., *La Privacy. Proteggere i dati personali oggi*, Bologna, 2015

FOGLIA C., *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione nel GDPR*, in PANETTA R. (a cura di), *Circolazione e protezione dei dati personali tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, 2019

GALETTA D.U., *La tutela dei diritti fondamentali (in generale, e dei diritti sociali in particolare) nel diritto UE dopo l'entrata in vigore del Trattato di Lisbona*, in *Rivista italiana di diritto pubblico comunitario*, Anno XXIII, Fasc. 5-6, 2013

GALIANO A., LEOGRANDE A., MASSARI S. F., MASSARO A., *I dati non personali: la natura e il valore*, in *Rivista italiana di informatica e diritto*, fasc. 1-2020

GARZONIO E., *L'algoritmo trasparente: obiettivi ed implicazioni della riforma dello Spazio digitale europeo*, in *Rivista italiana di informatica e diritto*, fasc. n. 2/2021

GARZONIO E., *Responsabilità degli ISP rispetto al trattamento automatizzato dei dati personali con finalità di comunicazione politica: applicabilità del GDPR alle piattaforme social*, in *MediaLaws*, n. 2/2019

GIANNONE CODIGLIONE G., *Risk-based approach e trattamento dei dati personali*, in SICA S., D'ANTONIO V., RICCIO G. M., *La nuova disciplina europea sulla privacy*, 2016

GOBBATO S., *Verso l'attuazione della direttiva (UE) 2019/1024 sul riutilizzo degli open data della PA: nuove opportunità per le imprese*, in *MediaLaws*, n. 2/2020

GONZALEZ FUSTER G., *The emergence of personal data protection as a fundamental right of the EU*, Springer, 2014

GRAEF I., GELLERT R., HUSOVEC M., *Towards a holistic regulatory approach for the European data economy: Why the illusive notion of non-personal data is counterproductive to data innovation*, in *TILEC Discussion Paper No. 2018-029*, 2018

GRUSCHKA N., MAVROEIDIS V., VISHI K., JENSEN M., *Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR, 2018 IEEE International Conference on Big Data (Big Data),* 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 *Dpce online*, 2/2017

HIJMANS H., *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU*, Law, Governance and Technology Series 31, Springer, 2016

HINTZE M., *Viewing the GDPR through a De-Identification Lens: A Tool for Compliance, Clarification, and Consistency*, in *International Data Protection Law*, *Oxford University Press*, Vol. 8, Issue 1, 2018

IANNUZZI A., FILOSA F., *Il trattamento dei dati genetici e biometrici*, in *Dirittifondamentali.it*, Fascicolo 2/2019

IANNUZZI A., *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale*, in *Studi parlamentari e di politica costituzionale*, Anno 54, n. 209, 2021

IRTI C., *Personal Data, Non-Personal Data, Anonymised Data, Pseudonymised Data, De-identified Data*, in SENIGAGLIA R., IRTI C., BERNES A. (eds.), *Privacy and Data Protection in Software Service*, Springer, 2022

KERBER W., *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, Joint Discussion Paper Series in Economics by the Universities of Aachen, Gießen, Göttingen, Kassel, Marburg, Siegen, No. 37-2016

KERBER W., SCHWEITZER H., *Interoperability in the Digital Economy*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (JIPITEC), *MAGKS, Joint Discussion Paper Series in Economics*, No. 12-2017, 2017

KIRSCHEN S., *Il trasferimento all'estero dei dati*, in PANETTA (a cura di), *Circolazione e protezione dei dati personali tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, 2019

KOOPS B.J., *The trouble with European data protection law*, in *International Data Privacy Law*, 2014

KUSIAK A., *A Four-part Plan for Smart Manufacturing*, in *ISE Magazine*, Vol. 49, No.7, 2017

KUSIAK A., *Fundamentals of smart manufacturing: A multi-thread perspective*, in *Annual Reviews in Control*, Vol. 47, 2019

KUSIAK A., *Smart manufacturing*, in *International Journal of Production Research*, 2018

LEISTNER M., *Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform*, in LOHSSE S., SCHULZE R.,

STAUDENMAYER D. (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools*, 2017

LI Y., *Cross-border Data Transfer Regulation in China*, in *Rivista italiana di informatica e diritto*, fasc. n. 1/2021

MAI J.-E., *Big data privacy: The datafication of personal information*, in *The Information Society*, Vol. 32, No. 3, 2016

MANTELERO A., *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era*, in TAYLOR L., FLORIDI L., VAN DER SLOOT B. (eds), *Group Privacy New Challenges of Data Technologies*, Springer, 2017

MANTELERO A., *From Safe Harbour to Privacy Shield. The "Medieval" sovereignity on pesonal data*, in *Contratto e Impresa/Europa*, 2016

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*, 2016

MANTELERO A., *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le Nuove Leggi Civili Commentate*, n. 1/2017

MARONGIU BUONAIUTI F., *La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I-bis"*, in *Cuadernos de Derecho Transnacional*, vol. 9, n. 2, 2017

MARTONI M., *Datificazione dei nativi digitali. Una prima ricognizione e alcune brevi note sull'educazione alla cittadinanza digitale*, in *federalismi.it*, n. 1/2020

MAYER-SCHÖNBERGER V., CUKIER K., *Big Data. A Revolution that will transform how we live, work, and think*, London, John Murray Publishers, 2013

MAYER-SCHÖNBERGER V., PADOVA Y., *Regime Change? Enabling Big Data through Europe's New Data Protection Regulation*, in *The Columbia Science & Technology Law Review*, 2016

MCAFEE A., BRYNJOLFSSON E., *Big data: the management revolution*, in *Harvard Business Review*, n. 10/2012

MIGLIETTI L., *Profili storico-comparativi del diritto alla privacy*, in *diritticomparati.it*, 2014

MONTAGNANI M. L., *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in *Mercato concorrenza regole*, a. XXI, n. 2, agosto 2019

MOURBY M., MACKEY E., ELLIOT M., GOWANS H., WALLACE S., BELL J., SMITH H., AIDINLIS S., KAYE J., *Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK*, in *Computer Law & Security Review*, 2018

NARAYANAN A., FELTEN E.W, *No silver bullet: De-identification still doesn't work*, 2014

NARAYANAN A., SHMATIKOV V., *Myths and Fallacies of Personally Identifiable Information*, in *Communications of the ACM*, vol. 53, no. 6, 2010

NINO M., *Il caso Datagate. I problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy*, in *Diritti umani e diritto internazionale*, vol. 7, 2013, n. 3

NOTO LA DIEGA G., *Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (JIPITEC), 2018

OHM P., *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, UCLA Law Review, Vol. 57, 2010

OROFINO M., *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in PANELLA L., *Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno. Quaderni Ordine Internazionale e Diritti Umani Editoriale Scientifica*, Napoli, 2018

OROFINO M., *FBI v. Apple: il caso è (forse) chiuso, ma le questioni di fondo rimangono apertissime*, in *Diritto Pubblico Comparato ed Europeo*, vol. 26, n. 2, 2016

OROFINO M., *La libertà di espressione tra Costituzione e Carte europee dei diritti. Il dinamismo dei diritti in una società in continua trasformazione*, Giappichelli, Torino, 2014

OROFINO M., *Minori e diritto alla protezione dei dati personali*, in OROFINO M., PIZZETTI F., *Privacy, Minori e cyberbullismo*, Giappichelli, Torino, 2018

OROFINO M., *Trattamento dei dati personali e libertà di espressione e di informazione*, in CALIFANO L., COLAPIETRO C. (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, Napoli, 2017

PAGNANELLI V., *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in *Rivista italiana di informatica e diritto*, fasc. n. 1/2021

PALUMBO A., *Il diritto all'autodeterminazione informativa. L'esperienza tedesca in materia di protezione dei dati personali*, Tesi di dottorato, Università degli studi di Milano-Bicocca, 2015/16

PARDOLESI R., *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in PARDOLESI R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003

PARISI N., *Funzione e ruolo della Carta dei diritti fondamentali nel sistema delle fonti alla luce del Trattato di Lisbona*, in *Il diritto dell'Unione europea*, a. XIV, fasc. 3, 2009

PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali, I, Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016

POLLICINO O., BASSINI M., *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in RESTA G., ZENO-ZENCOVICH V. (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Collana "Consumatori e Mercato", 2016

POLLICINO O., BASSINI M., *Commento all'art. 8 CdfUE*, in *Carta dei diritti fondamentali dell'Unione europea*, MASTROIANNI R., POLLICINO O., ALLEGREZZA S., PAPPALARDO F., RAZZOLINI O. (a cura di), Milano, 2017

POULLET Y., GUTWIRTH S., *The contribution of the Article 29 Working Party to the construction of a harmonised European dataprotection system: an illustration of 'reflexive governance'?* in PEREZ ASINARI M. V., PALAZZI P. (Eds) *Défis du droit à la protection de la vie privée. Challenges of privacy and data protection law - Challenges of privacy and data protection law*, 2008

PURTOVA N., *The Illusion of Personal Data as No One's Property*, in *Law, Innovation, and Technology*, 2015

PURTOVA N., *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, in *Law, Innovation and Technology*, Vol. 10, No. 1, 2018

RESTA G., *La "morte" digitale*, in *Il diritto dell'informazione e dell'informatica*, Anno XXIX, Fasc. 6-2014

RESTA G., *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in RESTA, ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Collana "Consumatori e Mercato", 2016

RICCIO G. M., *Model Contract Clauses e Corporate Binding Rules: valide alternative al Safe Harbor Agreement?*, in RESTA, ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Collana "Consumatori e Mercato", 2016

RODOTÀ S., *Data Protection as a Fundamental Right*, in GUTWIRTH S., POULLET Y., DE HERT P., DE TERWANGNE C., NOUWT S. (eds), *Reinventing Data Protection?*, Springer,2009

RODOTÀ S., *Il mondo nella rete – Quali diritti, quali vincoli*, Laterza, Bari, 2014

ROSE M., *Europe can win global battle for industrial data, EU industry chief says*, Reuters, 15-02-2020

ROSSI DAL POZZO F., *La giurisprudenza della Corte di giustizia sul trattamento dei dati personali*, in *Associazione Italiana Studiosi di Diritto dell'Unione europea* (AISDUE)*, Sezione "Convegni annuali e interinali"*, n. 9, 2019

RUBECHI M., *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *federalismi.it*, n. 23/2016

RUNSHAN H., STALLA-BOURDILLON S., YANG M., SCHIAVO V. SASSONE V., *Bridging Policy, Regulation, and Practice? A Techno-Legal Analysis of Three Types of Data in the GDPR*, in LEENES R., VAN BRAKEL R., GUTWIRTH S., DE HERT P. (eds), *Data Protection and Privacy: The Age of Intelligent Machines*, 2017

RUOTOLO G. M.*, I dati non personali: l'emersione dei big data nel diritto dell'Unione europea*, in *Studi sull'integrazione europea*, 2018

RYAN P.S., FALVEY S., MERCHANT R., *When the Cloud Goes Local: The Global Problem with Data Localization*, in *Computer*, Vol. 46, No. 12, 2013

SALERNO G. M., *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in NANIA R., RIDOLA P. (a cura di), *I diritti costituzionali*, vol. 2, Torino, 2006

SALERNO G. M., *Le garanzie della democrazia*, in *Rivista Associazione Italiana dei Costituzionalisti* n°: 3/2018

SARTOR G., *Tutela della personalità e normativa per la «protezione dei dati». La sentenza della corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici del «Datenschutz»*, in *Informatica e Diritto*, 1986

SAVELYEV A., *Russia's new personal data localization regulations: A step forward or a self-imposed sanction?*, in *Computer Law & Security Review: The International Journal of Technology Law and Practice,* 2015

SCHERMER B., *The limits of privacy in automated profiling and data mining,* in *Computer law & security review* 27, 2011

SCHNEIER B., *Schneier on Security, A blog covering security and security technology*, 2010

SCHWARTZ P., *Property, Privacy, and Personal Data*, in *Harvard Law Review*, 2004

SCHWARTZ P., SOLOVE D., *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, in *New York University Law Review*, Vol. 86, 2011

SIMONCINI A., *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 2019, 63 ss.

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

STALLA-BOURDILLON S., KNIGHT A., *Anonymous data v. Personal Data – A false debate: an EU perspective on anonymization, pseudonymization and personal data*, in *Wisconsin International Law Journal*, 2016

STANZIONE M. G., *Genesi ed ambito di applicazione*, in SICA S., D'ANTONIO V., RICCIO G., *La nuova disciplina europea della privacy*, 2016

SURBLYTE G., *Data as a Digital Resource*, in *Max Planck Institute for Innovation & Competition Research Paper No. 16-12*, 2016

SWIRE P., LAGOS Y., *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, in *Maryland Law Review* 335, 2013

TARANTINO L., *Promozione della concorrenza e disciplina dei servizi pubblici*, 2016

TENE O., POLONETSKY J., *Big Data for All: Privacy and User Control in the Age of Analytics*, in *Northwestern Journal of Technology and Intellectual Property*, Vol. 11, Issue 5, 2013

TIBERI G., Riservatezza e protezione dei dati personali, in CARTABIA M. (a cura di), *I diritti in azione*, Bologna, 2007

TJONG TJIN TAI E., *Data ownership and consumer protection*, Tilburg Private Law Working Paper Series No. 09/2017

TOMBAL T., *Economic Dependence and Data Access*, in *International Review of Intellectual Property and Competition Law* (IIC), Issue 51 (1), 2020

TRUCCO L., "*Data retention": la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giurisprudenza italiana*, 2014

ÜNVER H. A., KIM G., *Cross-Border Data Transfers and Data Localization*, EDAM Cyber Policy Paper Series 2016/3

URBIOLA P., *Data Flows Across Borders. Overcoming Data Localization Restrictions*, Institute of International Finance, 2019

URGESSA W., *The Protective Capacity of the Criterion of "Identifiability" Under EU Data Protection Law*, in *European Data Protection Law Review* (EDPL), vol. 2, no. 4, 2016

VALLE L., GRECO L., *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale*, in *Il diritto dell'informazione e dell'informatica*, Anno XXXII, Fasc. 2-2017

VAN DIJCK J., *Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology*, in *Surveillance and Society*, Vol. 12, No. 2, 2014

VICTOR J., *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, in *Yale Law Journal*, 2013

VOIGT P., VON DEM BUSSCHE A., *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, 2017

WARREN S.D., BRANDEIS L.D., *The right to privacy*, *Harvard Law Review*, 1890

WERNICK A., OLK C., VON GRAFENSTEIN M., *Defining Data Intermediaries – A Clearer View through the Lens of Intellectual Property Governance*, in *Technology and Regulation*, 2020

WESTIN A., *Privacy and Freedom*, New York: Atheneum, 1967

WIEBE A., *Protection of industrial data – a new property right for the digital economy?*, in *Journal of Intellectual Property Law & Practice*, 2016

WILKINSON M., DUMONTIER M., AALBERSBERG I., APPLETON G., AXTON M., BAAK A., BLOMBERG N., BOITEN J.-W., BONINO DA SILVA SANTOS L., BOURNE P., BOUWMAN J., BROOKES A., CLARK T., CROSAS M., DILLO I., DUMON O., EDMUNDS S., EVELO C., FINKERS R., GONZALEZ-BELTRAN A., GRAY A., GROTH P., GOBLE C., GRETHE J., HERINGA J., HOEN P., HOOFT R., KUHN T., KOK R., KOK J., LUSHER S., MARTONE M., MONS A., PACKER A., PERSSON B., ROCCA-SERRA P., ROOS M., VAN SCHAIK R., SANSONE S.-A., SCHULTES E., SENGSTAG T., SLATER T., STRAWN G., SWERTZ M., THOMPSON M., VAN DER LEI J., VAN MULLIGEN E., VELTEROP J., WAAGMEESTER A., WITTENBURG P., WOLSTENCROFT K., ZHAO J., MONS B., *The FAIR Guiding Principles for scientific data management and stewardship*, in *Scientific Data*, 2016

YUEXIN Z., *Cyber protection of personal information in a multi-layered system*, in *Tsinghua China Law Review*, n. 2/2019

ZHANG S., *Who owns the data generated by your smart car?*, in *Harvard Journal of Law & Technology* Volume 32, Number 1, 2018

ZARSKY T., *Incompatible: The GDPR in the Age of Big Data*, in *Seton Hall Law Review*, vol, 47, n. 995, 2017

ZECH H., *A legal framework for a data economy in the European Digital Single Market: rights to use data*, in *Journal of Intellectual Property Law & Practice*, 2016

ZENO-ZENCOVICH V., *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in RESTA, ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Collana "Consumatori e Mercato", 2016

ZENO-ZENCOVICH V., GIANNONE CODIGLIONE G., *Ten Legal perspectives on the "Big data revolution"*, in DI PORTO F. (a cura di), *Concorrenza e Mercato*, Numero speciale. Big Data e concorrenza, 2016

ZUIDERVEEN BORGESIUS F., *Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation*, in *Computer Law & Security Review*, 2016

ZWENNE G., *Diluted Privacy Law*, Universiteit Leiden, 2013

Normativa

Clarifying Lawful Overseas Use of Data Act, 2018

Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, n. 108 del 1981

Cybersecurity Law of the People's Republic of China, 2017

Data Security Law of the People's Republic of China, 2021

Decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla legge 18 novembre 2019, n. 133, "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica"

Decreto-Legge 30 aprile 2020, n. 28, convertito con modificazioni dalla legge 25 giugno 2020, n. 70, "Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19"

Decreto legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali"

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

Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati

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

Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»)

Direttiva 2001/29/CE del Parlamento europeo e del Consiglio, del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione

Direttiva 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

Direttiva 2003/58/CE del Parlamento europeo e del Consiglio, del 15 luglio 2003, che modifica la direttiva 68/151/CEE del Consiglio per quanto riguarda i requisiti di pubblicità di taluni tipi di società

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 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno

Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione

Direttiva (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

Direttiva (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 terrorismo e dei reati gravi

Direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti

Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico

Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1983), 25.03.1982

Legge 31 dicembre 1996, n. 675, “Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali”

Prima direttiva 68/151/CEE del Consiglio, del 9 marzo 1968, intesa a coordinare, per renderle equivalenti, le garanzie che sono richieste, negli Stati Membri, alle società a mente dell'articolo 58, secondo comma, del Trattato per proteggere gli interessi dei soci e dei terzi

Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla *governance* europea dei dati (Atto sulla governance dei dati), 25 novembre 2020 (Com(2020)767 final)

Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati), 23 febbraio 2022 (Com(2022)68 final)

Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE (COM(2020) 825 final)

Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali) (COM(2020) 842 final)

Provisional Agreement resulting from interinstitutional negotiations relativo alla Proposta di DGA (COM(2020)0767 – C9-0377/2020 – 2020/0340(COD)) del 15-12-2021

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 (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

Giurisprudenza

BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83

Cassazione civile, sez. II, 02/09/2015, sentenza n. 17440

Cassazione civile, sez. II, 05/07/2018, sentenza n. 17665

Corte di Giustizia, 12-11-1969, causa C-29/69, Stauder

Corte di Giustizia, 13-12-1979, causa C-44/79, Liselotte Hauer *c.* Land Rheinland-Pfalz

Corte di Giustizia, 20-5-2003, cause riunite C-465/00, C-138/01 e C-139/01, Rechnungshof *c.* Österreichischer Rundfunk e altri e Christa Neukomm e Joseph Lauermann *c.* Österreichischer Rundfunk

Corte di Giustizia, 6-11-2003, causa C-101/01, Lindqvist

Corte di Giustizia, 9-11-2004, causa C-46/02, Fixtures Marketing Ltd c. Oy Veikkaus Ab

Corte di Giustizia, 9-11-2004, causa C-203/02, The British Horseracing Board Ltd *c*. William Hill Organization Ltd

Corte di Giustizia, 9-11-2004, causa C-338/02, Fixtures Marketing Ltd *c*. Svenska Spel AB

Corte di Giustizia, 9-11-2004, causa C-444/02, Fixtures Marketing Ltd *c*. Organismos prognostikon agonon podosfairou AE (OPAP)

Corte di Giustizia, 29-1-2008, causa C-275/06, Promusicae

Corte di Giustizia, 9-11-2010, cause riunite C-92/09 e C-93/09, Volker und Markus Schecke GbR

Corte di Giustizia, 24-11-2011, causa C-70/10, Scarlet Extended SA *c*. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)

Corte di Giustizia, 24-11-2011, Cause riunite C-468/10 e C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) contro Administración del Estado

Corte di Giustizia, 8-4-2014, cause riunite C-293/12 e C-594/12, Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural resources et al.

Corte di Giustizia, 13-5-2014, causa C-131/12, Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González

Corte di Giustizia, 17-7-2014, cause riunite C-141/12 e C-372/12, YS *c.* Minister voor Immigratie, Integratie en Asiel, e Minister voor Immigratie, Integratie en Asiel *c*. M, S

Corte di Giustizia, 6-10-2015, causa C-362-14, Maximilian Schrems *c*. Data Protection Commissioner

Corte di Giustizia, 19-10-2016, causa C-582/14, Patrick Breyer *c*. Bundesrepublik Deutschland

Corte di Giustizia, 21-12-2016, cause riunite C-203/15 e C-698/15, Tele 2 Sverige AB *c*. Post-och telestyrelsen

Corte di giustizia, 9-03-2017, causa C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce *c*. Salvatore Manni

Corte di Giustizia, 20-12-2017, causa C-434/16, Peter Nowak *c*. Data Protection Commissioner

Corte di Giustizia, 16-07-2020, causa C-311/18, Data Protection Commissioner *c*. Facebook Ireland Limited e Maximillian Schrems

Corte europea dei diritti umani, Amann c. Svizzera (GC), n. 27798/95, 2000 - II

Corte europea dei diritti umani, Kopp c. Svizzera del 25 marzo 1998, Repertorio 1998-II

Corte europea dei diritti umani, Leander c. Svezia del 26 marzo 1987, Serie A n. 116

Corte europea dei diritti umani, Editorial Board of Pravoye Delo and Shtekel *c.* Ucraina del 5 maggio 2011

Documenti istituzionali

AGCM, AGCOM, Garante per la protezione dei dati personali, *Indagine conoscitiva sui big data*, 2018

Avvocato generale Cruz Villalón, Conclusioni del 12 dicembre 2013, Digital Rights Ireland Ltd (C-293/12) *c.* Minister for Communications, Marine and Natural Resources e altri e Kärntner Landesregierung (C-594/12) e altri

Comitato dei Ministri del Consiglio d'Europa, Risoluzione (73) 22 sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore privato, del 26/09/1973

Comitato dei Ministri del Consiglio d'Europa, Risoluzione (74) 29 sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore pubblico, del 20/09/197

Comitato economico e sociale europeo, Parere del Comitato economico e sociale europeo (CESE) sulla «Proposta di regolamento del Parlamento

europeo e del Consiglio relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea» (2018/C 227/12)

Comitato economico e sociale europeo, Parere del Comitato economico e sociale europeo (CESE) sulla "Comunicazione della Commissione al Parlamento europeo e al Consiglio - Linee guida sul regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea" adottato il 25 settembre 2019

Comitato europeo per la protezione dei dati (EBDB), Dichiarazione 05/2021 relativa all'atto sulla governance dei dati alla luce degli sviluppi legislativi, adottata il 19 maggio 2021

Comitato europeo per la protezione dei dati (EDPB), Garante europeo della protezione dei dati (GEPD), Parere congiunto EDPB-GEPD 03/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati), Versione 1.1 del 9-06-2021

Comitato europeo per la protezione dei dati (EDPB), Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 2018

Commission nationale de l'informatique et des libertés (CNIL), Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC

Commission nationale de l'informatique et des libertés (CNIL), *How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence*, 2017

Commissione europea, Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) (SWD(2020) 295 final)

Commissione europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Dati aperti Un motore per l'innovazione, la crescita e una governance trasparente (COM(2011) 882 final)

Commissione europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Verso una florida economia basata sui dati, (COM(2014) 442 final)

Commissione europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Strategia per il mercato unico digitale in Europa, (COM (2015) 192 final)

Commissione europea, *Commission staff working document on the free flow of data and emerging issues of the European data economy. Accompanying the document "Communication Building a European data economy"* (SWD (2017) 2 final)

Commissione europea, Comunicazione della Commissione, Scambio e protezione dei dati personali in un mondo globalizzato, (COM (2017) 7 final)

Commissione europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Costruire un'economia dei dati europea* (COM (2017) 9 final)

Commissione europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale, (COM (2017) 228 final)

Commissione europea, Commission staff working document impact assessment, Accompanying the document "Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union" (SWD (2017) 304 final, part 1/2)

Commissione europea, Commission Staff working document, *Evaluation of Directive 96/9/EC on the legal protection of databases* (SWD (2018) 147 final)

Commissione europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, "Una strategia europea per i dati" (COM(2020) 66 final).

Commissione europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, "Verso uno spazio comune europeo dei dati", (COM(2018) 232 final)

Commissione europea, Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Guidance on the Regulation on a framework for the*

free flow of non-personal data in the European Union (COM (2019) 250 final)

Commissione europea, Documento di lavoro dei servizi della Commissione, Orientamenti sulla condivisione dei dati del settore privato nell'economia europea dei dati che accompagna il documento Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "Verso uno spazio comune europeo dei dati" (SWD(2018)125 final).

Commissione europea, Inception Impact Assessment, Ref. Ares(2021)3527151 - 28/05/2021

Commissione europea, Raccomandazione (UE) 2018/790 della Commissione del 25 aprile 2018 sull'accesso all'informazione scientifica e sulla sua conservazione

Commissione europea, Regulatory scrutiny board opinion, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), (SEC(2020) 405),

Cross-border data flow in the digital single market: study on data location restrictions", FINAL REPORT. *A study prepared for the European Commission DG Communications Networks, Content & Technology by: Time.lex, Spark Legal Network and Tech4i2* (SMART 2015/0054)

Data Ethics Commission (*Datenethikkommission*), *Opinion of the Data Ethics Commission*, 2019

DELOITTE, Realising the economic potential of machine-generated, non-personal data in the EU. Report for Vodafone Group, 2018

European Union Agengy For Network And Information Security (ENISA), *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*, 2015

Federal Ministry for Economic Affairs and Energy (BMWi), *GAIA-X: A Pitch Towards Europe. Status Report on User Ecosystems and Requirements*, 2020

Garante europeo della protezione dei dati, *Opinion 3/2020 on the European strategy for data*, 16-06-2020

Garante per la protezione dei dati personali, Parere su una istanza di accesso civico - 10 gennaio 2019 (doc. web n. 9084520)

Garante per la protezione dei dati personali, Provvedimento in ordine all'applicabilità alle persone giuridiche del Codice in materia di protezione dei dati personali a seguito delle modifiche apportate dal d.l. n. 201/2011 (Pubblicato sulla Gazzetta Ufficiale n. 268 del 16 novembre 2012; Registro dei provvedimenti n. 262 del 20 settembre 2012)

Garante per la protezione dei dati personali, Provvedimento del 10 gennaio 2019, Registro dei provvedimenti n. 5 (doc. web n. 9080914)

Garante per la protezione dei dati personali, Provvedimento del 22 gennaio 2021, Registro dei provvedimenti n. 20 (doc. web n. 9524194)

Gruppo di lavoro Articolo 29, *Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers* (WP74)

Gruppo di lavoro Articolo 29, Linee guida sul diritto alla portabilità dei dati (WP 242) adottate il 13 dicembre 2016 e modificate il 5 aprile 2017

Gruppo di lavoro Articolo 29, Linee-guida sui responsabili della protezione dei dati (RPD) (WP 243) adottate il 13 dicembre 2016 e modificate il 5 aprile 2017

Gruppo di lavoro 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 (WP 248) adottate il 4 aprile 2017 e modificate il 4 ottobre 2017

Gruppo di lavoro Articolo 29, Opinion 05/2014 on Anonymisation Techniques (WP216) adottata il 10 aprile 2014

Gruppo di lavoro Articolo 29, Parere 4/2007 sul concetto di dati personali" (WP136) adottato il 20 giugno 2007

IDC 2017, *European Data Market Study*, Final Report (SMART 2013/0063)

Impact Assessment on enhancing the use of data in Europe. Report on Task 1 – Data governance, prepared for the European Commission (SMART 2020/694 | D2)

Information Commissioner Office (ICO), *Anonymisation: managing data protection risk code of practice*, 2012

Information Commissioner Office (ICO), *ICO analysis of the Council of the European Union text of the General Data Protection Regulation*

Irish Data Protection Commission, *Guidance on Anonymisation and Pseudonymisation*, 2019

ISO Smart Manufacturing Coordinating Committee, *White Paper on Smart Manufacturing*, 2021

National Board of Trade (Kommerskollegium), *No Transfer, No Trade: the Importance of Cross-Border Data Transfers for Companies Based in Sweden*, 2014

Organization for Economic Co-operation and Development (OECD), *Data-Driven Innovation: Big Data for Growth and Well-Being*, 2015

Organization for Economic Co-operation and Development (OECD), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, Paris, 2019

Organization for Economic Co-operation and Development (OECD), *Quality framework and guidelines for OECD statistical activities*, version *2011/1 (STD/QFS(2011)1)*

Organization for Economic Co-operation and Development (OECD), Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 23 settembre 1980 - C(80)58/FINAL

Organization for Economic Co-operation and Development (OECD), *Summary of the OECD privacy expert roundtable, Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*, 21-3-2014

Organization for Economic Co-operation and Development (OECD), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, in *OECD Digital Economy Papers*, No. 176, OECD Publishing, Paris, 2011

Parlamento europeo, Risoluzione sulla tutela dei diritti dell'individuo di fronte al crescente progresso tecnico nel settore dell'informatica, 8 maggio 1979

Parlamento europeo, Risoluzione sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto (2016/2225(INI)), 14 marzo 2017

Workshop on labels for or certification of providers of technical solutions for data exchange: Summary of discussions, del 12-05-2020

World Economic Forum, *Personal Data: The Emergence of a New Asset Class, An Initiative of the World Economic Forum In Collaboration with Bain & Company, Inc.*, 2011

World Economic Forum, *Rethinking Personal Data: A New Lens for Strengthening Trust, Industry Agenda prepared in collaboration with A.T. Kearney*, 2014