Intermediazione di dati personali e servizi di *data sharing* dal GDPR al *Data Governance Act*

Fabio Bravo

Sommario: 1. La strategia europea sui dati e l'emanazione della nuova proposta di Regolamento sulla *European data governance* (*Data Governance Act*). – 1.1. Dal GDPR alla Comunicazione della Commissione per una «Strategia europea sui dati». – 1.2. Il mutamento del linguaggio e il mutamento del paradigma: il «*titolare dei dati» (data holder*) e l'«*utilizzatore dei dati» (data user*). – 1.3. Dalla Comunicazione della Commissione sulla *European Strategy for Data* alla Proposta di regolamento sulla *European Data Governance*. – 2. Valore economico dei dati personali e loro commercializzazione nei nuovi modelli di *business* realizzati dagli "infomediari". Le esperienze di *data intermediation* nella prassi (casi Lumeria, Weople, ErnieApp) e i problemi giuridici emergenti, tra autonomia privata e GDPR. – 2.1. Dati personali, strumenti di potere e valore economico. – 2.2. Modelli di *business* basati su dati personali. L'*infomediazione* delle *data companies* tra autonomia privata e GDPR. – 2.3. (*segue*) *Il caso Lumeria.* – 2.4. (*segue*) *Il caso Weople.* – 2.5. (*segue*) *Il caso ErnieApp.* – 3. Commercializzazione di dati personali e contratti volti ad ottenere la loro "monetizzazione" mediante l'attività di "infomediari": criticità emergenti. – 4. I servizi di condivisione dei dati nella proposta di regolamento sulla *governance* europea dei dati *(Data Governance Act*). – 4.1. Servizi di *data sharing* e ruolo degli intermediari di dati al cospetto del mercato. – 4.2. «Titolare dei dati» e «utente dei dati». – 4.3. Caratteristiche, confini e funzioni del servizio di *data sharing*. – 4.4. Servizi di condivisione dei dati e tutela degli interessati. Conflitti di interesse e «incentivi disallineati». – 4.5. (*segue*) Gestione dei diritti dell'interessato e delega. – 4.6. (*segue*) Finalità esclu-

Abstract

This essay analyses the phenomenon of data intermediation, on which The European Commission has recently paid attention with the Communication on "European Strategy for Data" and with the Proposal of a specific EU Regulation on "European Data Governance" (Data Governance Act). In this (proposal of) Regulation there are specific provisions of law about file sharing services provided by data intermediaries and new roles are mentioned: "data holders", "data users" and "providers of data sharing services" (as data intermediaries between them). The European perspective is clear: to create or to sustain new business opportunities for European enterprises and advantages for Public Institutions, as well. This deep innovation arises new problems and needs to be considered in light of the existing data protection law and to be coordinated with the GDPR.

1. La strategia europea sui dati e l'emanazione della nuova proposta di Regolamento sulla *European data governance* (*Data Governance Act*)

1.1. *Dal GDPR alla Comunicazione della Commissione per una «Strategia europea sui dati»*

L'ordinamento giuridico europeo, dopo un lento percorso che ha portato al formale riconoscimento del diritto alla protezione dei dati personali nell'ambito della carta dei diritti fondamentali dell'UE (art. 8), sta percorrendo ora direzioni volte ad incoraggiare il mercato dei dati personali[1], al fine di non far perdere competi-

[1] Si rimanda, sul tema, ai contributi dell'intero volume *Persona e mercato dei dati. Riflessioni sul GDPR*, di a cura di Zorzi Galgano, Milano,

tività alle imprese europee di fronte alle logiche proprietarie che invece animano i mercati extraeuropei[2].

L'attenzione per il mercato dei dati personali e per le dinamiche concorrenziali nella fornitura dei servizi s'è già avvertita nelle scelte che hanno animato il Reg. (UE) n. 679/2016 (GDPR)[3]: si pensi, in particolare, al nuovo diritto alla *data portability*, nella parte in cui l'interessato ha la facoltà di chiedere ad un titolare dei dati di trasferire i dati personali direttamente ad altro titolare, in formato strutturato ed elettronico, leggibile da dispositivo, anche qualora il secondo titolare, indicato dall'interessato, sia un *competitor* del primo nella fornitura di un determinato servizio[4].

A distanza di meno di quattro anni dall'emanazione del GDPR ed a meno di un biennio dalla sua applicazione, che com'è noto decorre dal 25 maggio 2018, la Commissione europea ha sentito l'esigenza di emanare la Comunicazione intitolata «*Una strategia*

2019; nonché a Zeno Zencovich, *Do "data markets" exist?*, in *Media Laws*, 2019, 2, p. 22 ss.; Spiekermann, Acquisti, Böhme e Hui, *The challenges of personal data markets and privacy*, in *Electronic markets*, 2015, 25(2), p. 161-167.

[2] Per una lettura critica del ricorso al modello proprietario si veda Alpa, *La "proprietà" dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di Zorzi Galgano, cit., p. 11 ss.; ma v. anche Zeno Zencovich, *Do "data markets" exist?*, cit., p. 25 ss. (con riguardo al par. 3, intitolato ««*Ownership*" *of data*»); Singh, *Protecting Personal Data as a Property Right*, in *ILI Law Rev*., 2016, p. 123 ss., nonché Hugenholtz, *Data property: unwelcome guest in the house of IP*, in *Better Regulation for Copyright: Academics meet Policy Makers*, a cura di Reda, Brusselles, 2017, p. 65-77.

[3] Per un commento critico al Reg. (UE) n. 679/2016 si rinvia a *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di Zorzi Galgano, cit.; *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, a cura di Finocchiaro, Bologna, 2019; *I dati personali nel diritto europeo*, a cura di Cuffaro, D'Orazio e Ricciuto, Torino, 2019.

[4] Sul tema si vedano le osservazioni di S. Troiano, *Il diritto alla portabilità dei dati*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di Zorzi Galgano, cit., p. 195 ss.; Soimani, *The right to data portability and user control: ambitions and limitations*, in *Riv. dir. media*, 2018, 3, p. 2 ss.

europea per i dati» [COM(2020) 66 final del 19 febbraio 2020][5]: la spinta ad incentivare il mercato dei dati e a favorire una «sovranità tecnologica europea»[6] viene coniugata con una visione volta a far sempre salvo il principio personalistico[7]. In tale documento si legge anche lo scopo dell'azione annunciata dalla Commissione, ove la dimensione economica – vero obiettivo della strategia perseguita – non viene mai persa di vista: «l'Europa mira a sfruttare i vantaggi di un migliore utilizzo dei dati, compresi una maggiore produttività e mercati competitivi, ma anche miglioramenti in materia di salute e benessere, ambiente, amministrazione trasparente e servizi pubblici convenienti. Le misure illustrate nel presente documento contribuiscono a un approccio globale all'economia dei dati. La presente comunicazione delinea una strategia per le misure politiche e gli investimenti a sostegno dell'economia dei dati per i prossimi cinque anni»[8]. Le scelte strategiche si incentrano, tra l'altro, sulla *disponibilità* e sulla *condivisione* dei dati, su una maggior chiarezza concernente le facoltà di utilizzo dei dati, sulla *governance* dei dati, sulla creazione di *spazi comuni europei di dati*, sull'*interoperabilità* e sulla *qualità* dei *dati*.

1.2. *Il mutamento del linguaggio e il mutamento del paradigma: il «titolare dei dati»* (data holder) *e l'«utilizzatore dei dati»* (data user)

Proprio sulla disponibilità dei dati si inizia a vedere un cambio di paradigma nelle strategie dell'UE, amplificato dalla trattazione

---

[5] Comunicazione della Commissione europea del 19 febbraio 2020, intitolata «*Una strategia europea per i dati*» [COM(2020)86 final].

[6] Cfr. Commissione europea, *Una strategia europea per i dati*, cit., p. 6, ove si trova rimarcato che «[i]l funzionamento dello spazio europeo di dati dipenderà dalla capacità dell'UE di investire nelle tecnologie e nelle infrastrutture di prossima generazione, come pure nelle competenze digitali, ad esempio l'alfabetizzazione ai dati (*data literacy*). Ciò contribuirà a sua volta a rafforzare la *sovranità tecnologica dell'Europa* per quanto riguarda le tecnologie e le infrastrutture abilitanti fondamentali per l'*economia dei dati*».

[7] Cfr. Commissione europea, *Una strategia europea per i dati*, cit., p. 5.

[8] Commissione europea, *Una strategia europea per i dati*, cit., p. 1 s.

unitaria di categorie profondamente diverse l'una dall'altra, quali i dati personali e non personali. Vengono introdotti concetti nuovi per le categorie giuridiche soggettive dell'ordinamento europeo, quale il «*titolare dei dati*» («*data holde*r», nella versione inglese), anche là dove ci si riferisce a «*dati personali*», e ciò prelude all'emanazione di norme in cui si ridelineano gli assetti giuridici concernenti le facoltà di utilizzo dei dati medesimi[9]. Fino ad ora l'UE aveva sempre rifiutato di introdurre il concetto di "*titolarità*" direttamente riferito ai *dati*: non era considerato «*titolare dei dati*» né il soggetto a cui si riferisce il dato personale, indicato come «*interessato al trattamento di dati personali*» – o «*data subject*», nella versione inglese –, né il soggetto che predispone il trattamento dei dati personali per finalità legittime dal medesimo stabilite, indicato come «*titolare dei trattamento dei dati personali*» – o «*data controller*», nella versione inglese. Mai prima d'ora s'è voluto riferire il concetto di "titolarità" direttamente al dato (e non al trattamento) e ciò denota un cambio di paradigma che rischia di essere un preludio all'introduzione, per via normativa, di una reificazione dei dati personali, quali entità giuridicamente rilevanti *ex sé* più che quali attribuiti della persona.

Vero è che la versione linguistica inglese, a differenza di quella italiana, utilizza il sostantivo «*holder*» e non «*owner*», ma ciò segna pur sempre un mutamento significativo del registro linguistico, in favore di una certa disponibilità fattuale e giuridica del dato, destinato a circolare in una sorta di "reificazione", al cospetto della quale diviene funzionale anche l'altro sostantivo, quello di «*user*»[10].

In proposito mi sembra doveroso rimarcare la connessione tra linguaggio e paradigma di riferimento, all'interno delle scelte di sistema ed è interessante rileggere a tal fine, nella letteratura stranie-

---

[9] *Ibidem*, p. 7. Le espressioni «titolare dei dati» ed «utilizzatore dei dati», contenute nella Comunicazione cit., sono poi state riprese nella Proposta di regolamento europeo nota come *Data Governance Act*, del 25 novembre 2020, su cui si tornerà più diffusamente nel prosieguo.

[10] La versione spagnola («*titular de datos*»; «*usuario de datos*»), così come quella francese («*détenteur de données*»; «*utilisateur de données*») e tedesca («*Dateninhaber*»; «*Datennutzer*»), solo per citarne alcune, confermano le scelte lessicali presenti, rispettivamente, nella traduzione italiana e in quella inglese.

ra di settore, un passaggio significativo di Jacob M. Victor, ove ha proposto il termine «*data user*» per indicare sia il «*data controller*» (il titolare del trattamento), sia il «*data processor*» (il responsabile del trattamento), nell'ambito di un saggio eloquentemente intitolato «*The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*» (pubblicato sul *Yale Law Journal* nel 2013, quando il GDPR era ancora sotto forma di proposta) [11]. Nel prendere in esame le «*entities that collect or process data-which, for ease, I will call "data users"*»[12], Victor chiarisce che «*The draft Regulation distinguishes between data "controllers", which own and maintain databases, and data "processors", which process data on behalf of data controllers* [*Id*. art. 4(5)-(6)]. *Because most of the Regulation's principles apply to both types of entities, I have adopted the neutral term "data user"*»[13]. Si tratta però di precisazione terminologica che non pare dettata solo da esigenze di semplificazione del linguaggio, come apparentemente sembra giustificare l'autore, ma che a ben guardare, lungi dall'essere connotata da caratteristiche di "neutralità", pare imposta dall'esigenza di inquadrare meglio gli istituti in altro paradigma teorico ed interpretativo: quello che ruota intorno ai "*property rights*" ed al "*property regime*". Ed infatti Victor prosegue le sue considerazioni annotando, poco dopo, che «*Though the Regulation is framed in the fundamental-human-rights terms typical of European privacy law, this Comment argues that it can also be conceived of in property-rights terms. The Regulation takes the unprecedented step of, in effect, creating a property regime in personal data, under which the property entitlement belongs to the data subject and is partially alienable*»[14].

In altre parole, v'è la conferma che il ricorso alla nuova nomenclatura per i protagonisti del trattamento dei dati sia in realtà – oggi (nei testi istituzionali dell'UE) come allora (nella letteratura

---

[11] Victor, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, in *Yale Law Journal*, 123, No. 2, 2013, p. 513-529.

[12] Victor, *op. cit.*, p. 513.

[13] Victor, *op. cit.*, p. 513.

[14] Victor, op. cit., p. 515.

di settore poc'anzi citata) – funzionale ad una lettura destinata ad erodere progressivamente la centralità del principio personalistico verso chiavi di lettura più aderenti al "*Property Regime*" o ad altri inquadramenti teorici che prestino attenzione al mercato[15]. La precisazione terminologica che si trova nel contributo di Victor nel 2013, nel tempo ha finito così per influenzare anche il lessico della Comunicazione della Commissione europea, dedicata alla *Strategia europea sui dati* (del febbraio 2020), così come quello della Proposta di regolamento sulla *European Data Governance* (del novembre 2020), ove si fa ricorso all'espressione «*data user*» (utilizzatore dei dati) e, nelle medesime logiche, «*data holder*», tradotto nella versione linguistica italiana con "titolare dei dati"[16].

Il mutamento del registro linguistico è un chiaro segno dell'apertura verso un mutamento di paradigma nelle logiche di circolazione dei dati personali non certo estranee all'impianto normativo vigente. Nella Comunicazione cit., si noti, la Commissione precisa che «il *valore dei dati* risiede nel loro *utilizzo* e *riutilizzo*. I dati attualmente disponibili non sono sufficienti per un riutilizzo innovativo, ad esempio per lo sviluppo dell'intelligenza artificiale. Le problematiche, che possono essere raggruppate in base all'identità del *titolare dei dati* e a quella del loro *utilizzatore*, dipendono tuttavia anche dalla natura dei dati interessati (*dati personali*, dati non personali o *set* di dati misti che comprendono entrambe le tipologie) (…)»[17].

---

[15] Cfr. Zeno Zencovich, *Do "data markets" exist?*, cit., p. 25 ss., ove si precisa che « *Once data is under the control of a business there can be no doubt that it has the right to use, not use and exploit such data, being well aware that as that data is non-rival it might be in the availability also of some other entity: the typical example is that of statistical data acquired from a public body. Whether one uses trade secret rules, or the sui generis protection for data banks, whoever lawfully holds the data is entitled – therefore the term "entitlement" appears much more appropriate than ownership – to use them*».

[16] Si tratta però di traduzione non appagante perché suggerisce l'idea di una "*ownership*". Si veda, sulle scelte linguistiche, quanto riportato nella nota precedente.

[17] Commissione europea, *Una strategia europea per i dati*, cit., p. 7.

1.3. *Dalla Comunicazione della Commissione sulla* European Strategy for Data *alla Proposta di regolamento sulla* European Data Governance

L'indirizzo strategico non ha tardato a materializzarsi in proposte normative, emanate nella forma di proposte di regolamenti europei. L'UE ne ha pubblicate ben tre: la prima, del 25 novembre 2020, ha ad oggetto la disciplina della *European Data Governance*[18], seguita da altre due proposte di regolamento del 15 dicembre 2020, denominate rispettivamente «*Digital Markets Act*»[19] e «*Digital Services Act*»[20], volte a delineare un quadro competitivo nel mercato digitale europeo, nel quale i dati hanno un ruolo decisamente strategico[21].

Con riguardo a tali proposte di Regolamento si intende porre l'attenzione, nel presente contributo, su uno specifico tema relativo alla *governance* europea dei dati: quello concernente la fornitura del servizio di condivisione dei dati (personali). Viene cristallizzato, nella nuova proposta di regolamento, un modello di *business* già registrato nella prassi, basato sul ruolo dell'intermediario di dati (infomediario) che, nel fornire il servizio di *data sharing*, agisce come una sorta di *broker* "*sui generis*" tra "titolari del trattamento dei dati" e "interessato del trattamento"[22]. Nel *Data Governance Act*, come già preannunciato, si fa però ricorso – significativamente

---

[18] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European data governance* (*Data Governance Act*) [COM/2020/767 final], Bruxelles, 25.11.2020.

[19] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector* (*Digital Markets Act*) [COM/2020/842 final], Bruxelles, 15.12.2020.

[20] European Commission, *Proposal for a Regulation of the European Parliament and of the Council «on a Single Market For Digital Services* (*Digital Services Act*) *and amending Directive 2000/31/EC*» [COM/2020/825 final], Bruxelles, 15.12.2020.

[21] Cfr. Commissione europea, *Una strategia europea per i dati*, cit., p. 28.

[22] Per un'analisi delle questioni giuridiche concernenti l'infomediazione cfr. Bravo, *Il commercio elettronico dei dati personali*, in *Questioni attuali in tema di commercio elettronico*, a cura di Pasquino, Rizzo e Tescaro, Napoli, 2020, p. 83-130.

– ad altro registro linguistico, già anticipato nella Comunicazione sulla strategia europea dei dati, personali e non personali: il fornitore dei servizi di condivisione, anche quando opera nel mercato dei dati personali, mette in relazione il «*titolare dei dati*» («*data holder*») con l'«*utilizzatore dei dati*» («*data user*»), offrendo *servizi a valore aggiunto*, con cui la Commissione intende *scalfire il ruolo dominante assunto dalle multinazionali d'oltreoceano*[23]. Queste ultime si sono fatte largo tra le amplissime maglie della disciplina di favore accordata loro dalla normativa europea sul commercio elettronico, risalente ad inizio millennio (dir. 2000/31/CE sul commercio elettronico)[24] ma che appare ora destinata ad una significativa riforma, direttamente dal citato *Digital Services Act*, oltre che indirettamente, *ratione materiae*, anche dal *Digital Markets Act e* dal *Data Governance Act*.

Il presente contributo intende ripercorrere le questioni giuridiche che si pongono con riguardo al predetto modello di *business*, basato sulla figura degli intermediari di dati, al fine di vagliare criticamente le scelte normative contenute nella proposta di regolamento sulla *governance* europea dei dati, concernenti la disciplina del servizio di condivisione dei dati. L'analisi, ovviamente, non può non tener conto anche del sistema di protezione che l'UE ha già delineato in materia di protezione dei dati personali, con specifico riferimento al GDPR.

---

[23] Cfr. Commissione europea, *Una strategia europea per i dati*, cit., p. 3 s.

[24] La disciplina in materia di *e-commerce* (dir. 2000/31/CE) contiene norme minimali, volte a creare situazioni di esenzione da responsabilità nella fornitura di determinati servizi della società dell'informazione (*hosting*, *caching* e *mere conduit*) per consentire lo sviluppo del commercio elettronico, funzionale alla creazione di un mercato transfrontaliero basato sulle tecnologie digitali, senza intervenire su altri servizi e senza prevedere forme di vigilanza, né in fase di accesso al mercato (tant'è che viene escluso l'obbligo di un'autorizzazione preventiva per lo svolgimento delle attività di commercio elettronico: v. art. 3 dir. cit.), né in fase di svolgimento del servizio. Le proposte di regolamento rese negli ultimi mesi del 2020 rivoluzionano l'approccio, prevedendo forme di vigilanza nello svolgimento dei servizi della società dell'informazione.

2. Valore economico dei dati personali e loro commercializzazione nei nuovi modelli di business realizzati dagli "infomediari". Le esperienze di *data intermediation* nella prassi (casi Lumeria, Weople, ErnieApp) e i problemi giuridici emergenti, tra autonomia privata e GDPR

2.1. *Dati personali, strumenti di potere e valore economico*

I dati personali sono divenuti oggetto di crescente attenzione da parte di istituzioni e di imprese, per la straordinaria capacità di sviluppo che essi comportano. La possibilità di ricavare informazioni dalla loro analisi consente di godere di indiscutibili vantaggi in termini di potere e di controllo[25] in molteplici ambiti, tra cui quello del mercato (c.d. *business intelligence*, *behavioural advertising*)[26], quello finanziario (*FinTech*, *TechFin*)[27], quello politico (anche con riguardo alla manipolazione a fini elettorali)[28],

---

[25] Cfr. Rodotà, *Tecnologie e diritti*, Bologna, 1995, p. 34 ss.; Id., *Controllo e privacy della vita quotidiana. Dalla tutela della vita privata alla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 2019, 1, pp. 9 ss.; Mantelero, *Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Dir. inf.*, 2012, p. 135 ss.; Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization* (April 4, 2015), in *Journal of Information Technology* (2015) 30, 75–89.

[26] Bourreau, de Streel e Graef, *Big Data and Competition Policy: Market Power, Personalised Pricing and Advertising* (February 16, 2017), in SSRN: https://ssrn.com/abstract=2920301.

[27] Zetzsche, Buckley, Arner e Barberis, *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance (April 28, 2017)*, in *University of Hong Kong Faculty of Law Research Paper No. 2017/007*; *University of Luxembourg Law Working Paper No. 2017-001*, in SSRN: https://ssrn.com/abstract=2959925; *Fintech: diritto, tecnologia e finanza*, a cura di Lener, in *Quaderni di Minerva Bancaria*, Milano, 2018; *I diversi settori del Fintech. Problemi e prospettive*, a cura di E. Corapi e Lener, Milano, 2019; *Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, a cura di Finocchiaro e Falce, Bologna, 2019.

[28] La profilazione dei cittadini e l'uso strumentale dei *Big Data* in vista di elezioni politiche è messo in risalto, oltre che dal caso Facebook e Cambridge Analytica (su cui è intervenuto anche in nostro Garante per la

quello "governativo"[29]. I dati personali hanno inoltre una forte attitudine ad essere utilizzati in modelli di *business* profondamente redditizi[30], già esplorati nella prassi degli affari[31].

La Commissione europea, nella citata comunicazione sulla strategia per i dati, ha evidenziato che «Nel corso degli ultimi anni le tecnologie digitali hanno trasformato l'economia e la società, influenzando ogni settore di attività e la vita quotidiana di tutti i cittadini europei. I dati sono un elemento centrale di tale trasformazione, che non fa che cominciare. L'innovazione guidata dai dati genererà benefici enormi per i cittadini, ad esempio tramite il miglioramento della medicina personalizzata, le nuove soluzioni di mobilità e il suo contributo al *Green Deal* europeo. In una società in cui è in costante aumento la quantità di dati generati dai singoli cittadini, la metodologia di raccolta e utilizzo di tali dati deve porre al primo posto gli interessi delle persone, conformemente ai valori, ai diritti fondamentali e alle norme europei. I cittadini daranno fiducia alle innovazioni basate sui dati e le faranno proprie solo se saranno convinti che la condivisione dei dati personali nell'UE

---

protezione dei dati personali, con Provv. 10 gennaio 2019 n. 5, doc. web n. 9080914, e Provv. del 14 giugno 2019, n. 134, doc. web n. 9121486), anche dalla dottrina. Cfr., tra gli altri, Susser, Roessler e Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World* (December 23, 2018), in *Georgetown Law Technology Review*, Forthcoming, in SSRN: https://ssrn.com/abstract=3306006; Manheim e Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy* (October 25, 2018), in 21 *Yale Journal of Law and Technology* 106 (2019).

[29] Marthews e Tucker, *Government Surveillance and Internet Search Behavior* (February 17, 2017) in SSRN: https://ssrn.com/abstract=2412564; G. Resta, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Dir. inf.*, 2015, 4-5, p. 697 ss.; Zeno Zencovich, *Intorno al caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in *Dir. inf.*, 2015, 4-5, pp. 683 ss.

[30] È frequente, ad esempio, l'accostamento dei dati personali al "nuovo petrolio", per indicare le nuove opportunità commerciali che possono derivare, con forti guadagni, dal trattamento dei dati personali. Cfr. «*Personal Data: The "New Oil" of the 21st Century*», *panel discussion at World Economic Forum on Europe and Central Asia* 2011 (June 9, 2011).

[31] Cfr. Bravo, *Il commercio elettronico di dati personali*, cit., *passim*.

sarà soggetta in ogni caso alla piena conformità alle rigide norme dell'Unione in materia di protezione dei dati. Nel contempo, il volume crescente di dati industriali non personali e di dati pubblici in Europa, unito ai cambiamenti tecnologici riguardanti le modalità di conservazione ed elaborazione dei dati, costituirà una potenziale fonte di crescita e innovazione che è opportuno sfruttare»[32].

Nella costante tensione tra il perseguimento di interessi economici e il guadagno di competitività del mercato europeo, da un lato, e la tutela della persona, dall'altro lato, emerge una chiara presa d'atto della rilevanza, anche patrimoniale, dei dati personali.

Secondo alcune stime fatte nel mercato americano alla fine del secolo scorso – e dunque poco più di una ventina di anni fa – «*consumer marketers are currently paying between 10 cents and US$2.50 for profiles of consumers, often based on their zip code and buying habits*»[33], il che, rapportato al numero complessivo di persone di cui una *data company* tratta dati personali, ha fatto stimare, nel 1999, che «*these people digest $75 billion worth of customer information every year*»[34]. Attualmente le stime si aggirano fino a 50 $ circa per ciascun profilo[35] ed il numero complessivo di utenti, nei diversi servizi offerti su Internet, si è elevato in maniera esponenziale. Ad oggi l'esposizione *online* degli utenti e la fruizione dei servizi telematici è aumentata considerevolmente, così come sono

---

[32] Commissione europea, *Una strategia europea per i dati*, cit., p. 1.

[33] Sullivan, *How Much is Your Playlist Worth?*, in *Wired News*, 1999, 11th March and 3rd November, reperibile *online* sul sito www.wired.it.

[34] Sullivan, *How Much is Your Playlist Worth?*, cit.; Schwartz, *Property, Privacy, and Personal Data*, in 117 *Harv. L. Rev.*, 2003-2004, p. 2056, n. 1.

[35] Cfr., Zeno Zencovich, *Do "data markets" exist?*, cit., p. 23 e, ivi, anche nt. 2: «*At a very elementary level, before the Internet age, many companies were providing for a very small sum, information concerning the phone number or the whereabouts of a subscriber or of a business. Still now there is a flourishing market – especially in the medical sector and in the US – of personal data, which in certain cases can reach $50 per name* [*the Report by the US Federal Trade Commission, Data Brokers. A Call for Transparency and Accountability (May 2014). For the economic analysis of a series of new information markets see* D. Bergemann-A. Bonatti, *Markets for Information: An Introduction, Cowles Foundation Discussion paper no. 2142 (August 2018)*]».

altrettanto considerevolmente aumentate le capacità di raccolta e di calcolo dei dati riferiti agli utenti, che vengono ora analizzati con tecniche ancora più sofisticate in quanto basate su sistemi di intelligenza artificiale: ciò lascia ovviamente intendere che il "mercato" dei dati personali è in crescita e che le stime sopra riferite siano da considerare di gran lunga più elevate, se si tiene a mente che la sola Facebook, su scala globale, vanta ora ben «*2.603 bilion monthly active users* (MAU)» [36]. Inoltre, come precisato dall'AGCM in recenti provvedimenti sanzionatori di pratiche commerciali scorrette perpetrate tramite il noto *social network*, in riferimento proprio all'utilizzo di dati personali degli utenti, dopo aver rimarcato che Facebook Inc. e Facebook Ireland Ltd. sono rispettivamente capogruppo e società operativa a livello europeo, ha evidenziato che «Il fatturato consolidato di Facebook Inc., al 31 dicembre 2019, risulta pari a 62,931 miliardi di euro (fonte SEC, sulla base del tasso di cambio euro/dollaro al 31 dicembre 2019)»[37], mentre «Il fatturato di Facebook Ireland Ltd., al 31 dicembre 2019, risulta pari a 34,326 miliardi di euro»[38]. Si tratta di dati particolarmente significativi se confrontanti con l'altra evidenza, emersa in fase di istruttoria nei procedimenti dell'AGCM, ossia che «i ricavi provenienti dalla pubblicità *on line*, basata sulla profilazione degli utenti a partire dai loro dati, costituiscono l'intero fatturato di Facebook Ireland Ltd. e il 98% del fatturato di Facebook Inc»[39].

---

[36] Il numero è ripreso dalle statistiche aggiornate al 1° maggio 2020, riportate da Smith, *250 Amazing Facebook Statistics and Facts for 2020. By the Numbers*, in *DMR. Business Statistics*, 2010, 14th July (*last update*), consultabile all'url https://expandedramblings.com/index.php/by-the-numbers-17-amazing-facebook-stats/#3-facebook-user-statistics-and-demographics.

[37] AGCM, provv. del 9 febbraio 2021, p. 4, consultabile *online* all'url www.agcm.it/dotcmsdoc/allegati-news/IP330_chiusura.pdf.

[38] *Ibidem*.

[39] Cfr. AGCM, provv. del 29 novembre 2018, n. 27432, così come riportato da T.a.r. Lazio, Roma, sentt. 260 e 261 citt., par. 2 delle motivazioni in diritto, su cui v., *amplius*, Bravo, *La «compravendita» di dati personali?*, in *Diritto di Internet*, 2020, 3, p. 521-540.

Tutto ciò fa ben comprendere l'impatto che i dati personali hanno sul mercato.

Il loro indiscutibile valore economico non deve però portare a ritenere che i medesimi siano anche "beni giuridici" in senso tecnico, quale "merce" che forma oggetto di commercializzazione[40], rimanendo pur sempre attributi della personalità, sui quali è possibile l'esercizio di diritti, anche nel senso di un uso di carattere patrimoniale[41]. Ed infatti, anche in tale loro qualificazione che por-

---

[40] Il dibattito è risalente. Per tutti si rinvia a P. Perlingieri, *L'informazione come bene giuridico*, in *Rass. dir. civ.*, 1990, p. 326 ss.; Zeno Zencovich, voce *Cosa*, in *Dig. IV, disc. priv., sez. civ.,* 1990, spc. par. 13; D. Messinetti, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, p. 339 ss.; Zeno Zencovich, *Sull'informazione come bene (e sul metodo del dibattito giuridico)*, in *Riv. crit. dir. pr.*, 1999, p. 485 ss.; G. Resta, *L'appropriazione dell´immateriale. Quali limiti?*, in *Dir. inf.*, 2004, 1, pp. 21-48; Camardi, *Cose, beni e nuovi beni, tra diritto europeo e diritto interno*, in *Eur. e dir. priv.*, 2018, 3, pp. 955 ss., spt. nt. 16. Sull'inquadramento dei dati personali nella categoria di bene giuridico, inteso in senso ampio e non confinabile entro il perimetro dell'art. 810 c.c., si veda, recentemente, il contributo monografico di Angiolini, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, Torino, 2020. Sulla difficoltà di ricorrere alla categoria di bene in senso giuridico si veda anche la posizione di Camardi, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in *Giust. civ.*, 2019, 3, p. 499 ss., nt. 14; Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *I dati personali nel diritto europeo*, a cura di Cuffaro, D'Orazio e Ricciuto, cit., p. 24; Bravo, *Lo "scambio di dati personali" nella fornitura di servizi digitali ed il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e impresa*, 2019, 1, p. 34-58. In materia s'è pronunciato anche il Garante europeo per la protezione dei dati personali (EDPS), con proprio Parere n. 4/2017 del 17 marzo 2017, con cui, esprimendo critiche decise alle scelte legislative espresse con la proposta di direttiva sui contratti di fornitura di contenuti e servizi digitali, aveva sì riconosciuto l'esistenza di un "mercato" dei dati personali, ma aveva escluso che i dati medesimi potessero essere considerati quali oggetto di controprestazione nell'ambito di operazioni di scambio di beni e servizi rivolti a consumatori.

[41] Si vedano, in particolare, gli studi di G. Resta, *Autonomia privata e diritti della personalità*, Napoli, 2005, *passim*.

ta ad inquadrare i dati personali nell'ambito della tutela dei dritti della personalità – è indubbio che possano essere oggetto anche di forme di contrattualizzazione[42], pacificamente ammesse dalla giurisprudenza e dallo stesso legislatore europeo, ancorché con qualificazioni giuridiche non sempre appaganti[43].

2.2. *Modelli di* business *basati su dati personali. L'infomediazione delle data companies tra autonomia privata e GDPR*

Alcuni modelli di *business*, oggi abbondantemente percorsi nella prassi, si basano su operazioni di "scambio di dati", ossia su operazioni che prevedono la fornitura di servizi a titolo oneroso, con controprestazioni non monetarie, ma basate sull'accesso,

---

[42] *Ibidem*.

[43] Addirittura il T.a.r. Lazio, sent. nn. 260 e 261 del 10 gennaio 2020, non ha esitato a qualificare come «compravendita» di dati personali le operazioni con cui un interessato al trattamento dei dati personali concede l'utilizzo a fini economici dei dati al medesimo riferibili in cambio dei servizi informatici (in particolare di *social network*), senza alcuna richiesta di eseguire prestazioni pecuniarie. Il riferimento al tipo della compravendita non è tuttavia corretto (v., *amplius*, Bravo, *La «compravendita» di dati personali?*, cit., p. 521-540), ma cela il rischio di giungere a logiche di apprensione di tipo proprietario sui dati personali, che tuttavia non sembrano in linea con le scelte assunte dall'ordinamento europeo. Più equilibrate, invece, è la sentenza della Cass. n. 17278/2018, che, pur parlando di contratti aventi ad oggetto uno "scambio di dati" personali, ne fissa i limiti, lasciando comunque intendere la sussistenza della meritevolezza degli interessi perseguiti e, quindi, anche la liceità della causa, ai sensi dell'art. 1322, co. 2, c.c. in tema di autonomia contrattuale. Sul punto si veda Bravo, *Lo "scambio di dati personali" nella fornitura di servizi digitali ed il consenso dell'interessato tra autorizzazione e contratto*, cit., p. 34-58. Il problema dell'inquadramento giuridico dei contratti in questione è affrontato anche dal legislatore europeo, con scelte non del tutto convincenti: si confrontino, in particolare, il testo definitivo della dir. 770/2019 con quello della proposta di direttiva, su cui si vedano le serrate critiche di C. Camardi, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, cit., p. 499-523.

la comunicazione e l'uso, per fini economici, dei dati personali dell'interessato[44], con impiego in un "doppio mercato"[45].

Altri modelli di *business* fanno leva sempre sul trattamento di dati personali degli utenti, ma sono impostati su logiche diverse, riconducibili al fenomeno della c.d. *infomediation*, ove le *data companies* si propongono – almeno formalmente – di agire in favore e per conto degli interessati, di cui acquisiscono una mole impressionante di dati, al fine di ottenere, presso fornitori terzi, la produzione di valore economico-monetario, che viene trasferito agli stessi previa decurtazione di una quota, destinata a remunerare i servizi resi dalla *data company* "infomediaria" [46].

---

[44] V. nota precedente, nonché G. Resta e Zeno Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. e proc. civ.*, 2018, 2, p. 411 ss.; Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, cit., p. 23 ss. e p. 45 ss.; Bravo, *Il commercio elettronico dei dati personali*, cit., *passim*.

[45] Cfr. Zeno Zencovich, *Do "data markets" exist?*, cit., p. 10, ove si rimarca che «*now it is finally accepted that provision of digital services on the Internet generally generates a two-sided market. The provider collects data from users and sells targeted advertisement services to business that want to reach certain groups. However, this is not always true, i.e. not all data markets are two-sided*».

[46] Cfr., *amplius*, Hagel e Rayport, *The Coming Battle for Customer Information*, in *Harvard Business Review*, January-February, 1997, ove si rinvengono significative e profetiche considerazioni: «*We believe that consumers are going to take ownership of information about themselves and demand value in exchange for it (…). Consumers probably will not bargain with vendors on their own, however. We anticipate that companies we call infomediaries will seize the opportunity to act as custodians, agents and brokers of customer information, marketing it to businesses on consumers' behalf while protecting their privacy at the same time*». Cfr. anche Hagel e Rayport, *The new infomediaries*, in *The McKinsey Quarterly*, Autumn 1997, p. 54 ss. Le *infomediaries* sono dunque società che si propongono di raccogliere informazioni sul comportamento dei consumatori per poi cederle a titolo oneroso, a società che intendano utilizzarle solitamente per finalità di *marketing*, ma anche, come è avvenuto nel celebre caso Cambridge Analytica (v. *supra*, nt. 28), per finalità di condizionamento elettorale in ambito politico ed altre.

2.3. (segue) *Il caso Lumeria*

La ricerca di nuovi *business models* nel settore dell'*infomediation* ha quindi indotto le *infomediaries*, successivamente, a spostare l'attenzione verso la fornitura di servizi direttamente ai consumatori, come nel caso di Lumeria, società californiana operante già dalla fine del secolo scorso nel settore dell'*identity management* e della *consumer privacy*, che, tra i propri servizi, forniva alle persone fisiche strumenti per proteggere e condividere i propri dati personali, agendo in nome e per conto dei singoli interessati, quale loro rappresentante, al fine di proteggere i loro dati personali ed estrarre valore da tali dati, che venivano memorizzati in appositi *database* gestiti da tale società[47].

Una volta raccolti in tal modo i dati personali dei clienti e creati dei "superprofili" con grandi quantità di dati *(big data*), appetibili per le società interessate ad attingervi per finalità di *marketing*, la società intermediaria curava i rapporti commerciali con soggetti terzi, interessati ad avere accesso a tali dati e a utilizzarli per scopi commerciali, a fronte di un corrispettivo che, nel modello di *business* delineato da Lumeria, giungeva direttamente ai soggetti interessati, suoi clienti, tranne che per una quota, che veniva invece trattenuta dalla società di intermediazione per la remunerazione della propria attività[48]. La società di intermediazione di dati ave-

---

[47] Cfr. Lester, *The Reinvention of Privacy*, in *The Atlantic*, 2001, March, ove viene illustrata l'operatività delle *new infomediaries* e, in particolare, di Lumeria.

[48] Il funzionamento di tali aspetti del modello di *business* di Lumeria è descritto da Lester, *The Reinvention of Privacy*, cit.: «*A customer will store personal data in what is called a SuperProfile. The more specific the information stored (about such things as age, sex, family status, sexual orientation, income level, assets, consumer preferences, and current shopping interests), the more valuable that profile will become to advertisers, who will pay handsomely to participate in Lumeria's network. They will do this because Lumeria will give them the chance to do highly targeted, permission-based marketing — to offer special deals on, say, new cars or house-painting services or plane tickets — exclusively to people of a predetermined demographic profile, and often only to people who have already expressed an interest in the very things being advertised. Most of the money from advertisers will go*

va altresì la funzione di consentire ai soggetti interessati, propri clienti, di selezionare quali, tra i molteplici dati personali raccolti nei propri *database*, mettere di volta in volta in condivisione con i fornitori, consentendo agli interessati medesimi di esercitare determinate forme sofisticate di controllo sui propri dati, avvalendosi di strumenti tecnologici di interazione.

2.4. (segue) *Il caso Weople*

Il predetto modello di *business*, due decenni dopo, è apparso anche in Italia, sulla spinta dell'introduzione del diritto alla portabilità dei dati ad opera del Reg. UE n. 679/2016 (GDPR): paradigmatico è il caso del servizio denominato «Weople», offerto dalla società milanese Hoda srl, che si propone oggi, in Italia, di offrire servizi di *infomediation* analoghi a quelli lanciati circa venti anni orsono da Lumeria –, sollevando subito l'attenzione del Garante per la protezione dei dati personali che, in una lettera alquanto allarmata, ha chiesto all'EDPB (*European Data Protection Board*) una disamina congiunta per una soluzione europea alle questioni giuridiche, di grande impatto per i diritti e le libertà degli interessati, che tale modello comporta[49].

Come si evince dal sito Internet relativo al servizio Weople (https://weople.space), l'idea di fondo, declamata nella homepage, è quella di costituire «La prima Banca per investire e recuperare valore dai tuoi dati, proteggerli e agire i tuoi diritti di *privacy*. Gratis e senza sforzo».

Al di là delle declamazioni, che potrebbero apparire, se non decettive, quantomeno oggetto di evidente forzatura (ad esempio ove si fa riferimento al concetto di pretesa "gratuità" e a quello dell'assenza di sforzo, che non favoriscono la comprensione della reale portata dell'operazione giuridica ed economica e inducono

---

directly to Lumeria's users; Lumeria will take a small cut».

[49] Cfr. Lettera del Presidente del Garante per la protezione dei dati personali al Presidente dell'*European Data Protection Board* (EDPB), avente ad oggetto «*Richiesta di parere in tema di commercializzazione dei dati personali e diritto alla portabilità*» (Garante per la protezione dei dati personali, doc web n. 9126725 del 1° agosto 2019.

ad una sottovalutazione dei rischi che possono gravare sui diritti e le libertà degli interessati), il servizio si basa, innanzitutto, sul «*caveau* personale», definita nell'app Weople come «cassetta di sicurezza», ove i singoli interessati possono depositare i propri dati personali già trattati da altri provider, quali ad esempio «i dati relativi agli account social, i dati delle spese effettuate con le carte fedeltà personali, i dati delle spese online tramite gli account e-commerce, i dati posseduti da Google e Apple (…)»[50].

Con l'attivazione dell'*account* Weople, in altre parole, l'interessato delega il *provider* a richiedere una copia dei dati personali ai diversi altri *provider*, concentrando nel "*caveau*" tutte le numerose informazioni di carattere personale già trattate da altri fornitori, da Facebook ad Amazon, da WhatsApp a Gmail e Google Search, da iCloud a Dropbox, e così via[51].

Il servizio si basa, sotto il profilo giuridico, sull'esercizio del diritto alla portabilità dei dati, previsto dall'art. 20 del Reg. (UE) n. 679/2016, che consente agli interessati non solo di richiedere per sé la disponibilità dei propri dati personali, in formato elettronico e strutturato, di uso comune e leggibile da dispositivo automatico, ai titolari del trattamento a cui l'interessato li abbia forniti, ma anche di trasferire tali dati ad altro titolare del trattamento o, addirittura, di ottenere dal primo titolare la trasmissione di tali dati direttamente all'altro titolare del trattamento, se tecnicamente fattibile,

---

[50] Cfr. la pagina «*Funzionalità*», sul sito Internet del servizio Weople, consultabile all'url https://weople.space/#come-funziona.

[51] Nella predetta pagina «*Funzionalità*» di Weople (v. nota precedente), si legge – con riguardo a «Come agisce Weople» – che «Attivare una cassetta di sicurezza significa avviare la procedura per ottenere una copia dei tuoi dati digitali. Weople agirà per te, chiederà i dati a chi li possiede e ti comunicherà non appena saranno disponibili. Inoltre, potrai monitorare costantemente lo stato di questa procedura dall'*app*. (….) All'inizio la cassetta di sicurezza è grigia, vuota e pronta per l'attivazione. Una volta attivata, cioè inserito l'*account* personale, la cassetta avrà il bordo azzurro, ma i dati sono in attesa e Weople li chiederà a chi attualmente li possiede. Quando i dati saranno in afflusso, la cassetta diventerà azzurra ed inizierà il vero e proprio investimento».

anche qualora si tratti di soggetti che svolgono attività concorrenziali tra loro[52].

Invero la norma del regolamento europeo – l'art. 20, par. 2, del GDPR – non richiede che il titolare del trattamento destinatario della trasmissione dei dati sia un soggetto che svolga un'attività analoga al primo o che i dati debbano essere trattati per le medesime finalità. Valgono a tal riguardo i principi generali.

Rispetto al dettato normativo, qui la richiesta di portabilità prevista in Weople giungerebbe direttamente dal secondo titolare, destinatario della trasmissione diretta, che agirebbe per conto dell'interessato, nella dichiarata prospettiva di valorizzarne i dati personali, con il suo consenso, ottenendo da fornitori terzi delle entrate in denaro e altri vantaggi.

Il servizio Weople prevede infatti, in primo luogo, la monetizzazione dei dati personali attraverso la funzionalità «Salvadanaio personali». Stando alla descrizione presente sul sito Internet di lancio del servizio, «In questo salvadanaio Weople verserà quanto le aziende pagheranno per mandarti una pubblicità e/o un'offerta di prodotti o servizi personalizzati. Il valore in Euro ti verrà messo a disposizione tramite sistemi di pagamento digitali e potrai usarlo come vorrai». Sono poi previsti ulteriori benefici, come le "offerte personalizzate", che i fornitori terzi potranno veicolare agli interessati tramite il servizio Weople, e le "vincite ad estrazione"[53].

Il servizio prevede poi anche funzioni di gestione dei diritti dell'interessato, come il diritto di rettifica o di revoca del consenso verso gli altri titolari del trattamento o gli altri diritti dell'interessato previsti dal regolamento europeo. Nella pagina del sito Internet

---

[52] Cfr. S. Troiano, *Il diritto alla portabilità dei dati personali*, cit., p. 199; A. Ricci, *I diritti dell'interessato*, in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, a cura di Finocchiaro, cit., p. 436 ss.;

[53] Nella pagina «*Funzionalità*» del servizio, sul sito Internet di Weople, viene a tal riguardo precisato che con «Le Vincite ad estrazione (…) Weople produrrà valore aggiunto investendo masse di dati, anonimi e protetti, nel mercato. Il valore generato dall'insieme verrà utilizzato per comprare premi da distribuire al maggior numero di persone possibili tramite più estrazioni durante l'anno».

relativa alle funzionalità del servizio Weople si trova scritto, infatti, che «Weople si offre di aiutarti a esercitare i tuoi diritti, veicolando le tue richieste presso aziende verso cui deciderai di agire e avvisandoti quando la richiesta sarà andata a buon fine (…)»[54], con l'avvertenza che non sarà sempre facile ed immediato l'esercizio di tali diritti: «Nonostante la legge a favore delle persone, il sistema si dovrà adattare e Weople avrà un compito non facile, almeno in una prima fase: sarà un percorso, Weople dovrà spingere, ridurre le resistenze, invocare la legge e trovare le strade migliori per fare arrivare sistematicamente i tuoi dati nel tuo conto ed esercitare i diritti come da [te] richiesto. Ecco una ragione in più per essere tanti e avere così un maggiore potere di pressione, per farci sentire e avere davvero la possibilità di far rispettare i nostri diritti»[55].

A dire il vero, come preannunciato, le prime resistenze sono venute proprio dal Garante per la protezione dei dati personali, che ha aperto un'istruttoria sulle modalità di trattamento relative al servizio Weople, interessando anche l'*European Data Protection Board* (EDPB), a garanzia dei diritti e delle libertà dell'interessato. Nella citata lettera di trasmissione della richiesta di parere in tema di commercializzazione dei dati personali e diritto della portabilità, indirizzata dal Presidente del Garante per la privacy al Presidente dell'EDPB (doc web n. 9126725 del 1° agosto 2019), viene testualmente precisato che «(…) si tratta di una questione molto rilevante che, pur venuta in evidenza in Italia, impone una riflessione generale che non può essere rimessa alle singole autorità di protezione dati. Il caso riguarda l'applicazione del diritto alla portabilità dei dati: un'impresa italiana si è infatti proposta come intermediaria nel rapporto fra titolari ed interessati chiedendo, su delega di questi ultimi, di ottenere le informazioni personali custodite presso importanti soggetti imprenditoriali, in particolare nel settore della grande distribuzione al fine di riunirle all'interno di una propria banca dati da sottoporre ad *enrichment*. Il tema è dun-

---

[54] V. pagina «*Funzionalità*», sul sito Internet del servizio Weople, il cui indirizzo è stato riportato nelle note precedenti.

[55] Cfr., ancora una volta, la pagina «*Funzionalità*» del sito Internet relativo al servizio Weople (già cit. nelle note precedenti).

que legato alla "commerciabilità" dei dati, con l'ulteriore complicazione dell'esercizio per delega del diritto ed il conseguente non remoto rischio di possibili duplicazioni delle banche dati oggetto di portabilità (…)».

Su tale questione il Garante ha anche diramato, in pari data, un Comunicato stampa (doc web n. 9126709 del 1° agosto 2019), intitolato «Dati in cambio di soldi: il Garante *privacy* porta la questione in Europa. Sotto la lente dell'Autorità la *app* "Weople"», con cui evidenzia le proprie perplessità, nonché l'allarmismo generato – si noti bene – non tanto dagli stessi interessati, ma dalle numerose imprese che, nella loro qualità di titolari del trattamento, hanno ricevuto le richieste di trasferimento dei dati in favore della società fornitrice del servizio Weople[56].

Si comprende bene, dunque, l'impatto che tale modello di business ha sulle dinamiche concorrenziali ed è proprio da questa esperienza che sembra essere germinata la strategia europea basata sull'intermediazione dei dati e sul servizio di *data sharing*, considerato nel *Data Governance Act*. Ed infatti nel predetto comunicato stampa, dopo aver premesso che «Con una lettera a firma del Presidente Antonello Soro, l'Autorità Garante per la privacy ha posto all'attenzione del Comitato europeo per la protezione dei dati personali (EDPB) la questione relativa a "Weople", l'*app* che promette ai propri iscritti una remunerazione in cambio della cessione dei loro dati personali (…)», si legge che «A partire dai primi mesi del 2019 sono state diverse le segnalazioni giunte all'Autorità da parte di imprese della grande distribuzione che lamentavano di aver ricevuto da parte di "Weople" numerosissime richieste di trasferire alla piattaforma dati personali e di consumo registrati nelle carte di fedeltà. L'impresa italiana, che gestisce la *app* e offre servizi di vario genere (offerte commerciali, analisti statistiche e di mercato), si propone infatti come intermediaria nel rapporto tra aziende e utenti chiedendo, su delega di questi ultimi, di ottene-

[56] Cfr. Comunicato del Garante per la protezione dei dati personali, doc web n. 9126709 del 1° agosto 2019, intitolato « *Dati in cambio di soldi: il Garante privacy porta la questione in Europa Sotto la lente dell'Autorità la app "Weople"*».

re le informazioni personali custodite presso grandi imprese allo scopo di riunirle all'interno della propria banca dati. L'attenzione del Garante si è concentrata, in particolare, sulla corretta applicazione, da parte della società, del cosiddetto diritto alla "portabilità dei dati" introdotto dal nuovo Regolamento europeo, con l'ulteriore complicazione determinata dall'esercitare tale diritto mediante una delega e con il conseguente rischio di possibili duplicazioni delle banche dati oggetto di portabilità. L'altro aspetto segnalato dal Garante nella lettera riguarda il delicato tema della "commerciabilità" dei dati, causata dall'attribuzione di un vero e proprio controvalore al dato personale. Su entrambe le questioni, il Garante ha dunque chiesto al Comitato, che riunisce tutte le Autorità Garanti dell'Unione, di pronunciarsi (...)».

Quanto al coinvolgimento dell'EDPB, il Comunicato del Garante rimarca che l'«attività di "Weople" (…) può produrre effetti in più di uno Stato dell'Unione in ragione delle richieste di portabilità che potranno essere avanzate e delle questioni relative alla "valorizzazione economica dei dati personali ed alla natura 'pro-concorrenziale' del diritto alla portabilità". Per questi motivi, pur essendo emerso in Italia, il caso della *app* impone (…) una riflessione generale che è più opportuno condividere con le altre Autorità di protezione dati. Il Garante attenderà dunque il parere dell'EDPB per concludere l'istruttoria avviata sulla *app*. Nel frattempo, i soggetti privati che riceveranno le richieste di portabilità dei dati da parte di "Weople" dovranno operare nel rispetto del principio di *accountability* stabilito dal Regolamento Ue e valutare se ottemperare alle richieste o motivare un eventuale rifiuto».

2.5. (segue) *Il caso ErnieApp*

Che si tratti di una questione destinata ad una rilevanza al di fuori del perimetro nazionale è ben evidente non solo perché tale *busness model* era stato già percorso negli Stati Uniti alla fine del secolo scorso dalla società californiana Lumeria[57], ma anche perché società attive nel settore dell'*infomediation* sono attualmen-

[57] V. *supra*.

te operanti anche dall'estero, com'è ad esempio per la ErnieApp Limited, che ha sede legale formalmente a Dublino[58], pur mantenendo un evidente collegamento con l'Italia, che si evince da tre indici: il servizio viene fornito sia in inglese che in italiano[59], l'amministratore delegato della società sembra essere di nazionalità italiana e vi è il coinvolgimento dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati[60]. Il servizio «ErnieApp» viene erogato via web o tramite un'*app*, che può essere scaricata sui principali *app store* (per Ios e per Android).

I servizi offerti e il modello di *business* sono – seppur con talune rilevanti differenze – analoghi a quelli di Weople (così come, in precedenza, di Lumeria), per ciò che riguarda: *a)* la gestione della *privacy* per conto dell'interessato, incluso l'esercizio dei diritti in materia di protezione dei dati personali (ad iniziare dalla gestione della manifestazione e della revoca del consenso, nonché di alti *privacy setting*); *b)* la commercializzazione dei dati, mediante attività volte a "monetizzare", per l'interessato, il consenso al trattamento dei dati personali rilasciato in favore di fornitori terzi.

---

[58] Cfr. il sito Internet del servizio ErnieApp, consultabile all'url https://ernieapp.com, nonché la pagina relativa alle «FAQ», ove viene precisato che la sede della società è a Dublino, in Irlanda, e che «*The service is now available in Argentina, Australia, Austria, Belgium, Bolivia, Bulgaria, Canada, Chile, Colombia, Croatia, Cyprus, Czech Republic, Denmark, Ecuador, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Israel, Lithuania, Latvia, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Paraguay, Peru, Poland, Portugal, Saudi Arabia, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, Turkey, United Kingdom, United States, Uruguay*».

[59] Sul sito del servizio ErnieApp, nella pagina delle FAQ, viene chiarito che «*ErnieApp has been released in English and Italian. We are working with partners to make the app available in several languages*».

[60] Sul sito viene evidenziato che il CEO di ErnieApp Limited è Isabella de Michelis di Slonghello, coautrice con Luca Bolognini, presidente dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati, dell'articolo intitolato «*An Introduction to the Right to Monetize (RTM)*», pubblicato online sul sito di ErnieApp il 9 aprile 2018, https://ernieapp.com/privacy-is-a-right-the-right-to-choose/.

Il fornitore del servizio (ErnieApp Limited), dunque, si propone formalmente come un «*Privacy Knowledge Manager* (PKM)», specificando – sul prorprio sito Internet – che «*A PKM empowers you to control how internet companies monetize your data based on the "consent" you provided them (the sharing permission you agreed to). User consent is usually collected upon sign-in to a digital service and at other times but users often underestimate what consent means. For digital companies your consent means a granted right to make a business with your data* (…)»[61]. Sicché ErnieApp interviene proprio nella gestione dinamica del consenso, fornendo in qualsiasi momento all'interessato uno strumento volto: (i) a rendere l'utente maggiormente consapevole delle implicazioni che la manifestazione del consenso ha per i fornitori dei servizi della società dell'informazione; (ii) a gestire nel tempo la manifestazione del consenso al trattamento dei dati personali nei confronti di diversi *providers*, nonché l'eventuale revoca del consenso; (iii) a ottenere un compenso in denaro, per l'utente, a fronte del consenso al trattamento dei dati personali prestato in favore di società terze, fornitrici dei servizi della società dell'informazione. La descrizione del servizio, nell'*homepage* del sito, così prosegue: «(…) *So with Ernieapp you can learn that your consent is important and that you have a right to change it, anytime you want (from Yes to No). Your decision to let a company use your personal data is so yours that you can also delete your personal data or request to be excluded from targeting advertisement and companies will have to accept it. So you are powerful! You can claim a fairer treatment from companies and just by managing your consent. ErnieApp gives you this opportunity. To manage dynamically your consent in exchange for good behavior from digital companies*»[62].

---

[61] Cfr. la descrizione del servizio ErnieApp sulla *homepage* del sito https://ernieapp.com. Quanto al diritto del titolare del trattamento a trattare dati personali degli interessati nell'ambito della propria attività economica e a trarre i relativi utili, cfr. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018, *passim*.

[62] Cfr. l'*homepage* del sito ErnieApp, https://ernieapp.com.

La descrizione del servizio non risulta particolarmente approfondita per ciò che riguarda le caratteristiche tecniche e le concrete funzionalità, ma – almeno stando ad una prima disamina – non sembra emergere l'esercizio del diritto alla portabilità dei dati personali dell'utente per l'acquisizione diretta dei dati medesimi presso fornitori terzi. Pare invece che il servizio sia basato sull'instaurazione di accordi con i *providers* terzi[63], al fine di interfacciare le funzionalità di controllo rilevanti in materia di protezione dei dati personali con il pannello di controllo reso disponibile nel servizio ErnieApp[64].

Ovviamente il potere di negoziazione del singolo utente, di fronte ai *providers* che richiedono di trattare dati personali, è estremamente basso, sicché il modello di *business* funziona allorché il "mediatore" sia in grado di far aderire al servizio una significativa massa critica di utenti, al fine di negoziare l'erogazione dei compensi in denaro con i singoli *providers*, sulla base degli accordi che verranno stipulati dal "mediatore" operante nel mercato dei dati personali[65].

---

[63] Sul sito del servizio ErnieApp, nella pagina FAQ (https://ernieapp.com/faq/), viene precisato che «*At the moment, the services we support are Google (e.g. Search, Maps), You Tube, Facebook, Instagram and Twitter. More services and more settings are on the pipeline and we will add them progressively giving to consumers further ways to exercise their rights*».

[64] V., ancora, la pagina FAQ del servizio ErnieApp (https://ernieapp.com/faq/), ove si legge che «*The Privacy Knowledge Manager is designed to make it easy for you to manage, across your digital accounts, the privacy settings of 3rd party applications, through a single dashboard (Home), in real time. By "manage" we mean enabling a change in the state of your 3rd party privacy settings (open/close/delete), including when we don't have a partnership with that given 3rd party. Usually these services have functions to enable changes to the privacy settings but in most cases the pages where these actions can be performed are hidden. In other application settings are not even available. While GDPR says they should. At ErnieApp we want to make easy for people to change their consent and permissions level on 3rd parties. So we designed an app which allows to do it with a click and allows also to compare between the internet services that are more user friendly than others* (…)».

[65] Si vedano, in proposito, le ulteriori precisazioni contenute sul sito

Le questioni giuridiche che si pongono, nei casi di *infomediation*, oltre all'ammissibilità o meno dell'operazione economica, sotto il profilo contrattuale e sotto il profilo della disciplina in materia di protezione dei dati personali, riguardano anche i rimedi e gli strumenti giuridici di protezione per evitare violazioni irreparabili dei diritti e delle libertà degli interessati.

3. Commercializzazione di dati personali e contratti volti ad ottenere la loro "monetizzazione" mediante l'attività di "infomediari": criticità emergenti

Quanto al modello di commercializzazione dei dati personali che poggia sull'attività di *informadiation*, vanno operati dei distinguo.

Le *new infomediaries* operano infatti secondo diversi modelli.

Qualora l' "infomediario" acquisisca direttamente i dati personali dell'interessato per conto del quale si propone di agire, facendoseli trasferire da altre *data companies* (come Facebook, Google, Apple, etc.) con ricorso al diritto alla portabilità dei dati previsto all'art. 20 GDPR – secondo il modello commerciale portato avanti da Lumeria e, ora, da Weople –, le questioni giuridiche che si dipanano sono molteplici e particolarmente delicate, tant'è che, come già evidenziato, si è subito allertato il Garante per la protezione dei

---

relative al servizio ErnieApp: «*End users, by exercising such right collectively, may create a consistent bargaining power, whereby today, as single individuals, they would not be able to achieve (…). Users' data in today's digital world are the raw material used to design and build most of the digital services and products that we know and use, including those to come in the near future, based on Artificial Intelligence (AI). End-users cannot be excluded, as they are today, from the data monetization opportunity as a consequence of the predominant technology stack design. End-users are too important to the value creation process to be excluded. Thus, it's time to create a proper policy framework to enable end-users to take advantage of this incredible opportunity. And by doing so, we will have a fairer, inclusive and more prosperous Internet ecosystem*». Così de Michelis di Slonghello e Bolognini, *An Introduction to the Right to Monetize (RTM)*, 9 aprile 2018, in https://ernieapp.com/privacy-is-a-right-the-right-to-choose/.

dati personali, aprendo un'istruttoria (ancora in corso) e coinvolgendo l'EDPB per adottare soluzioni condivise a livello europeo.

Vi è innanzitutto la questione relativa alle modalità di utilizzo del diritto alla portabilità dei dati personali a fini di commercializzazione dei dati medesimi. In dottrina è stata rimarcata la "valenza polifunzionale"[66] di tale diritto, in grado, per un verso, di esaltare «al massimo livello il potere dell'interessato di controllo sui dati»[67], rappresentando in tal modo «l'espressione più piena del diritto alla protezione dei dati personali nella sua proiezione positiva»[68]; per altro verso, invece, lo stesso diritto alla portabilità si pone in maniera fortemente *dinamica* come fattore propulsivo della libera circolazione dei dati, che ha la sua iniziale giustificazione nell'incentivazione del mercato e delle dinamiche concorrenziali, ma che, a ben guardare, presenta innegabili controindicazioni, con effetti collaterali ben diversi da come erano stati immaginati dal legislatore europeo[69]. Non solo emerge con forza il rischio della *commodification* dei dati personali (e con esso il processo di rei-

---

[66] Cfr. S. Troiano, *Il diritto alla portabilità dei dati personali*, cit., p. 199; A. Ricci, *I diritti dell'interessato*, cit., p. 436.

[67] S. Troiano, *Il diritto alla portabilità dei dati personali*, cit., p. 199.

[68] S. Troiano, *Il diritto alla portabilità dei dati personali*, cit., p. 199. Al riguardo l'A. rimarca che «il diritto alla portabilità dei dati si colloca in linea di continuità rispetto all'impostazione su cui è stato tradizionalmente eretto il sistema di tutela dei dati personali, sin dalla dir. n. 46 del 1995, ponendosi come strumento di massimo potenziamento del controllo sui dati ed evidenziando, pertanto, la sua natura di diritto fondamentale dell'interessato, al pari degli altri diritti di cui si costituisce l'evoluzione, ad iniziare, appunto, dal diritto di accesso. È questa la prospettiva fatta propria, in prima battuta, anche dal *considerando* n. 68 del Regolamento generale, che fa espresso riferimento all'esigenze di rafforzare il potere di controllo dell'interessato sui propri dati personali. Si tratta dunque dell'espressione precipua del diritto all'autodeterminazione informativa, trovando il suo fondamento nella garanzia sancita dall'art. 8 della Carta dei diritti fondamentali dell'Unione Europea (…)».

[69] Sui rischi generati dal principio di portabilità dei dati, inserito nel GDPR, al di là dell'idea di incentivare il mercato dei dati personali e la loro circolazione anche in una logica concorrenziale, sono stati ben evidenziati da S. Troiano, *Il diritto alla portabilità dei dati personali*, cit., p. 195 ss. e, ivi, spc. pp. 200-201, 209-211.

ficazione della persona) [70], ma anche le dinamiche concorrenziali sono tutt'altro che scontate[71]. In altre parole, anche in forza della facilità di spostamento di grandi quantità di dati e delle scelte di incentivazione della circolazione degli stessi ad opera del legislatore europeo con l'art. 20 del GDPR, si sta andando incontro ad un fenomeno di concentrazione *monopolistica* (oppure oligopolistica) dei dati personali[72].

---

[70] Cfr. S. Troiano, *Il diritto alla portabilità dei dati personali*, cit., p. 201, ove si rimarca che «consentendo, ed anzi promuovendo, il reimpiego dei dati da parte dell'interessato e il suo trasferimento a nuovi titolari del trattamento, si assecondi una logica di *commodification* dei dati quali oggetto (prima ancora che di protezione) del godimento e dello sfruttamento da parte dell'interessato, per finalità che possono essere indifferentemente di natura personale o economica. Si rafforza, dunque, una visione patrimonialistica e obiettivizzata dei dati personali, che ne offusca la funzione precipua di momenti di esplicazione della personalità dell'individuo». V. anche F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2017, p. 399, per il quale il diritto alla portabilità implica «il riconoscimento di un tipico potere di disposizione, qual è la prerogativa di cedere a terzi il diritto di sfruttamento di un'entità su cui si possa esercitare un controllo che prevale sull'altrui interesse all'utilizzazione in esclusiva».

[71] Le perplessità sul diritto alla portabilità dei dati, con riguardo alle dinamiche concorrenziali, sono state avanzate da Swinge e Lagos, *Why the right to data portability likely reduces consumer welfare: antitrust and privacy critique*, in *Maryland L. Rev.*, 2013, 72, p. 335 ss.; Weber, *Data portability and big data analytics. New competition policy challenges*, in *Concorrenza e mercato*, 2016, p. 59 ss.; S. Troiano, *Il diritto alla portabilità dei dati personali*, cit., p. 207.

[72] In dottrina si è avvertito che «è vero che la portabilità può consentire di rimuovere le barriere di mercato generate dal già menzionato effetto di *lock-in*, eliminando gli impedimenti che, ponendo ostacolo allo spostamento dei dati personali da una piattaforma ad un'altra, accrescono i costi e gli svantaggi del cambio di operatore e precludono l'accesso ai nuovi *providers*. Tuttavia, l'impiego del diritto alla portabilità dei dati come strumento di promozione della concorrenza non è privato di significativi profili problematici, in quanto, essendo sostanzialmente svincolato nei suoi presupposti e nel suo concreto operare dalle consolidate basi su cui è creato il diritto *antitrust*, rischia di produrre conseguenze indesiderate e controproducenti proprio nella specifica prospettiva del diritto

Il potere di controllo dell'interessato sui propri dati personali, tuttavia, sembra dileguarsi o esistere solamente in senso formale, dato che comunque, per poter essere esercitato, occorre che vi sia una infrastruttura tecnica e tecnologica, elemento indefettibile oggi per l'effettivo esercizio di un controllo sui dati. In un contesto sostanzialmente tecnocratico, qual è quello che si sta delineando attualmente [73], l'effettivo potere di controllo non risiede, come vorrebbe il legislatore, nelle mani dell'interessato, ma in quelle del titolare del trattamento che esercita il potere di predisposizione dell'apparato tecnologico per il trattamento dei dati e che, tramite esso, è in grado di utilizzare tali dati per finalità commerciali e di controllo sociale e, come s'è visto, anche politico[74].

Profetiche sono dunque le parole di un'attenta dottrina, con cui ha ammonito sui rischi inerenti alla portabilità dei dati sotto il profilo della tutela della persona, dato che, a prescindere dalle questioni relative alle dinamiche concorrenziali, «l'altro versante di critica riguarda la compatibilità di questo strumento e la stessa fondamentale istanza di proteggere la sfera personale dell'interessato dalle aggressioni esterne»[75].

---

della concorrenza». Così S. Troiano, *Il diritto alla portabilità dei dati personali*, cit., p. 207-208. V'è qui da aggiungere che gli effetti indesiderati, osservati dall'applicazione del diritto alla portabilità dei dati personali, si estendono in maniera pesante dal piano concorrenziale a quello dei diritti della personalità, che rischiano di essere gravemente compromessi.

[73] Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, p. 27 ss., 33 ss. e 59 s.

[74] V., *supra*.

[75] Così S. Troiano, *Il diritto alla portabilità dei dati personali*, cit., pp. 209 ss., ove evidenzia, a tal proposito, i rischi per la tutela della persona derivanti dalla migrazione da una piattaforma che garantisca maggiori livelli di protezione ad una connotata da un livello di protezione inferiore, nonché il rischio di un incremento delle ipotesi di violazione e furto dei dati in conseguenza della diffusione degli strumenti di interoperabilità richiesti per l'attuazione del diritto alla portabilità dei dati e, infine, il rischio di violazione del principio di minimizzazione dei dati, che va considerato come principio fondante e basilare della disciplina europea in materia di protezione dei dati personali («il diritto alla portabilità nella misura in cui persegue l'obiettivo di massimizzare la trasferibilità dei

Il problema è che, nel regolamento europeo (GDPR), non sono stati previsti argini al diritto alla portabilità, tanto con riguardo alle distorsioni sul piano concorrenziale, quanto sul piano della tutela dei diritti della persona. Si ravvisano gli estremi per un intervento regolativo delle Autorità di Controllo in materia di protezione dei dati personali, avvalendosi semmai anche degli strumenti di cooperazione e del c.d. meccanismo di coerenza previsti dal GDPR[76], per integrare il regolamento con atti di normazione secondaria (provvedimenti generali), eventualmente in sinergia con le autorità competenti in materia *antitrust*[77].

Tra i correttivi da apportare, sicuramente va considerata la previsione di un argine alla concentrazione dei dati personali, secondo criteri da definire. Si tenga però conto che, al di là del problema specifico legato all'esercizio del diritto alla portabilità, il tema è comunque rilevante con riguardo all'evidente accumulo di dati personali che già avviene da parte dei *Big Player* operanti nel settore IT, da Facebook (con l'omonimo *social network* e con WhatsApp) a Google (con i diversi servizi quali, tra cui Google Search Engine, Google Maps, YouTube, etc.), da Apple ad Amazon, e così via.

Ulteriori correttivi che meriterebbero di essere considerati dovrebbero riguardare la gestione del conflitto di interessi che potrebbe verificarsi in capo all'infomediario. Questi interagendo con

---

dati, si pone in irrimediabile conflitto con lo spirito di fondo a cui tali altri diritti dell'interessato invece coerentemente rispondono, ossia con l'esigenza, appunto, di minimizzazione dei dati e dei connessi rischi del trattamento»).

[76] Sui poteri dell'autorità di controllo delineati dai nuovi assetti normativi in materia di protezione dei dati personali e sulla cooperazione a livello europeo si vera il contributo di Busia, *Il ruolo dell'autorità indipendente per la protezione dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di Zorzi Galgano, cit., p. 293 ss. e 338 ss.

[77] V., *infra*, quanto osservato sul dialogo avviato da alcuni anni tra Garante per la protezione dei dati personali, Autorità garante per la concorrenza e il mercato ed Autorità per le garanzie delle comunicazioni, che ha portato ad un'indagine conoscitiva in materia di *Big Data* e ad un documento contenente specifiche linee guida, con raccomandazioni e *policy* in materia.

le *data companies* e altri soggetti terzi (nei cui confronti commercializza non solo i dati personali degli utenti, ma anche servizi a valore aggiunto rispetto ai dati grezzi raccolti), potrebbe essere indotto a sacrificare le logiche di protezione dei diritti e delle libertà degli interessati (che con la delega sembrerebbe invece condividere) per favorire gli interessi economici propri e della propria clientela, legati all'incremento di redditività, nonché il raggiungimento degli obiettivi della clientela *business* dell'infomediario, a cui vengono forniti i servizi a valore aggiunto. Si tratterebbe di obiettivi non prevedibili a priori nella sua portata, ma che potrebbero non essere ben compresi, nelle sue implicazioni, da parte degli interessati, come accaduto nel rapporto tra Facebook e Cambrige Analytica, su cui il Garante è intervenuto con propri provvedimenti[78].

Per la verità in Italia il Garante per la protezione dei dati personali, unitamente all'Autorità Garante della concorrenza e del mercato (AGCM) ed a quella per le garanzie nelle comunicazioni (AGCOM), hanno già avviato una sinergia in materia di *big data,* portata avanti dapprima con un'indagine conoscitiva del 20 maggio 2017 e successivamente con delle Linee Guida e Raccomandazioni di *Policy* in tema di *Big Data* del luglio 2019[79]. In esse, tuttavia, il tema dei rischi per le dinamiche concorrenziali e per le sue ricadute sul piano dei diritti fondamentali della persona non

[78] Cfr. Garante per la protezione dei dati personali, Provv. 10 gennaio 2019 n. 5, doc. web n. 9080914, e Provv. del 14 giugno 2019, n. 134, doc. web n. 9121486.

[79] AGCM, AGCOM e Garante Privacy, *Big Data. Indagine conoscitiva congiunta. Linee Guida e Raccomandazioni di Policy*, Roma, luglio 2019, disponibile all'url www.garanteprivacy.it/documents/10160/0/Big+Data.+Linee+guida+e+raccomandazioni+di+policy.+Indagine+conoscitiva+congiunta+di+Agcom%2C+Agcm+e+Garante+privacy.pdf/563c7b0e-adb2-c26c-72ee-fe4f88adbe92?version=1.1. Come chiarito in un comunicato stampa congiunto, presente anche sul sito del Garante per la protezione dei dati personali (doc web 9123066 del 10 luglio 2019), «Il documento è il frutto dell'indagine conoscitiva avviata congiuntamente dalle tre Autorità con l'obiettivo di comprendere le implicazioni – per la *privacy*, la regolazione, la tutela della concorrenza e del consumatore – dello sviluppo di un'economia digitale fondata sulla raccolta e analisi di una mole sempre più ingente di dati.

pare essere stato colto dalle predette *Authorities*, se si pensa che il rischio per le dinamiche concorrenziali emerge chiaramente con riguardo al problema della concentrazione tra le imprese, ma non dei dati in sé[80] e che, per altro verso, il diritto alla portabilità è stato ritenuto unicamente quale fattore incentivante le dinamiche concorrenziali, senza che si siano visti i rischi di un effetto opposto, evidenziati dalla dottrina e dalla prassi[81].

---

[80] Al punto n. 8 delle Linee Guida cit., le *Authorities* (Garante privacy, AGCM e AGCOM) hanno ritenuto di adottare, quale Policy-Raccomandazione, quella di «*Riformare il controllo delle operazioni di concentrazioni al fine di aumentare l'efficacia dell'intervento delle autorità di concorrenza*», rimarcando che «Con la diffusione dei Big Data, il controllo delle concentrazioni assume una nuova centralità. Al fine di aumentare l'efficacia dell'intervento delle autorità di concorrenza rispetto alle operazioni di concentrazione è auspicabile: 1. una riforma a livello nazionale e internazionale che consenta alle autorità di concorrenza di poter valutare pienamente anche quelle operazioni di concentrazione sotto le attuali soglie richieste per la comunicazione preventiva, ma che potrebbero risultare idonee a restringere sin dalla loro nascita importanti forme di concorrenza potenziale (come le acquisizioni da parte dei grandi operatori digitali di *start-up* particolarmente innovative anche soprannominate "*killing acquisitions*"); 2. la modifica dell'art. 6, comma 1, della legge n. 287/90, con l'introduzione di uno standard valutativo più adatto alle sfide dell'economia digitale, che faccia leva sul criterio dell'impedimento significativo della concorrenza effettiva (SIEC – "*Substantial impediment to effective competition*")». Non v'è però alcuna considerazione sugli effetti pregiudizievoli per la concorrenza in ordine alla concentrazione dei dati personali.

[81] Al punto n. 9 delle Linee Guida cit., infatti, le tre *Authorities* italiane (Garante privacy, AGCM e AGCOM) hanno puntato sul preteso effetto concorrenziale derivante dall'esercizio del diritto alla portabilità dei dati, sottovalutando l'effetto opposto, di cui non vi è traccia nel documento in questione. Così, viene raccomandato di «*Agevolare la portabilità e la mobilità di dati tra diverse piattaforme, tramite l'adozione di standard aperti e interoperabili*», dal momento che, secondo le predette istituzioni e in sintonia con lo spirito che ha portato, in sede europea, ad innovare la disciplina in materia di protezione e libera circolazione dei dati personali, «Agevolare la portabilità e la mobilità di dati tra diverse piattaforme, tramite l'adozione di standard aperti e interoperabili, anche oltre quanto già previsto dal diritto alla portabilità di cui all'art. 20 del RGPD, costituisce

Sicuramente utile è invece l'idea – delineata al punto n. 11 delle predette Linee Guida – di istituire un "*comitato permanente*" tra le tre *Authorities* domestiche, che potrebbe costituire un interessante tavolo di confronto per comprendere meglio i diversi aspetti che la fattispecie presenta e per pianificare più adeguate linee di intervento, avendo riguardo alle connessioni evidenti tra mercato e persona[82].

Altra questione, con riguardo al predetto modello di commercializzazione dei dati personali, concerne poi l'esercizio della delega da parte dell'informediario, come risulta – sempre a titolo esemplificativo – dall'art. 17 («*Conferimento di delega in favore di Hoda*») delle condizioni generali del servizio Weople (gestito da Hoda srl)[83], ove si trova stabilito che «Al fine di facilitare la procedura di esercizio del diritto, l'utente può assegnare a Hoda una delega per gestione della corrispondenza con i titolari del trattamento e, ove pertinente rispetto al contenuto della Richiesta, la ricezione

---

un *obiettivo con una forte valenza pro-concorrenziale* (…)». Proseguendo su tale linea si è poi addirittura considerato, ivi, che «In casi particolari, ferma restando la necessità di tutelare il diritto alla protezione dei dati personali, la tutela della concorrenza potrebbe richiedere obblighi di mobilità e portabilità dei dati personali ulteriori rispetto a quelli previsti in generale dal RGPD. A questo riguardo, si dovrebbe considerare la possibilità di estendere lo strumento della portabilità dei dati, oltre quanto – meritoriamente – stabilito dall'articolo 20 del RGPD, prevedendo una disciplina della portabilità dei dati, che favorisca lo sviluppo della competizione nei vari ambiti di valorizzazione economica del dato e, di conseguenza, una più efficace tutela del consumatore-utente. Possono pertanto essere prese in considerazione iniziative legislative o regolamentari, nell'ambito della cooperazione con l'Unione Europea, per disciplinare l'interoperabilità delle piattaforme tecnologiche, così da consentire effettivamente all'utente una piena portabilità dei propri dati».

[82] Al punto n. 11 delle cit. Linee Guida, viene proposta l'«*Istituzione di un "coordinamento permanente" tra le tre Autorità*», al rilievo che «Un'efficace politica pubblica per i Big Data e l'economia digitale richiede non solo l'*enforcement*, ma anche un'adeguata attività di *advocacy* di cui l'iniziativa congiunta tra AGCM, AGCom e Garante per la protezione dei dati personali è testimonianza (…)».

[83] Cfr. il documento intitolato «*Termini e condizioni generali per l'utilizzo di Weople*», disponibili all'url https://weople.space/terms#estese.

dei dati in seguito alla richiesta di portabilità di cui all'Art. 20, par. 2, GDPR (…)», con l'ulteriore precisazione che «La delega perde efficacia se l'utente sospende le proprie attività di investimento o elimina il proprio account».

Va chiarito che il diritto alla portabilità dei dati può essere esercitato non solo ottenendo per sé il trasferimento dei propri dati personali in formato elettronico, strutturato e leggibile da dispositivo, ma anche il trasferimento diretto da un titolare del trattamento ad un altro, a prescindere dalla delega. Sicché, anche in assenza della delega, l'infomediario potrebbe ottenere i dati personali dell'interessato attraverso una richiesta di trasferimento diretto, da questi avanzata ai sensi dell'art. 20, par. 2, del GDPR. Il meccanismo della delega, in questo modello di *business*, è chiaramente indirizzato a facilitare la concentrazione dei dati nell'infomediario, necessaria non solo per l'erogazione dei servizi a valore aggiunto da erogare alla clientela *business* verso cui si commercializzano i dati personali, ma anche per accreditarsi come soggetto privilegiato (avente posizione dominante sul mercato) con cui interloquire per i servizi in questione, ma produce l'effetto di concentrare, su un unico *provider*, diversi «*Big Data*» ottenuti da singoli diversi fornitori, già di per sé rilevanti quanto a concentrazione di dati, anche se isolatamente considerati.

Ciò genera un rischio evidente sotto diversi profili: innanzitutto perché finirebbero per convergere non solo i dati trattati dai fornitori dei servizi della società dell'informazione (*Internet service providers*), ma anche i dati sanitari trattati da istituti di cura e enti ospedalieri, nonché i dati economici trattati da istituti di credito, istituti di pagamento e società di intermediazione finanziaria, e così via, esponendo a rischi palesi l'interessato, non solo in caso di eventuale *data breach* o in caso di acquisizioni o fusioni societarie che coinvolgono l'attuale intermediario, ma anche durante l'operatività del servizio, in quanto l'*infomediario*, agendo per conto di soggetti terzi, utilizzerebbe comunque i predetti dati con il consenso dell'interessato al fine di incrementare la redditività sui dati andando a soddisfare via via le richieste degli operatori economici (e politici) interessati a trarre utilità da tale bacino informativo, senza tuttavia che l'interessato abbia sufficiente contezza di come

i dati vengano effettivamente utilizzati dai destinatari finali delle informazioni e per quali finalità.

Se si tengono bene a mente i requisiti del consenso, che deve essere "informato", "specifico", "inequivoco" e "libero", secondo anche il criterio della "granularità" (con l'applicazione che ne ha fatto la Corte di Cassazione, nella sent. n. 17278/2018, cit.), si comprende bene che il modello di *business* sopra evidenziato pone delicate questioni anche per ciò che attiene alle condizioni di liceità del trattamento, potendosi dubitare che possa essere ritenuto sufficiente il consenso al trattamento fornito all'*infomediario*, dovendosi invece verificare, nella casistica concreta, se l'interessato abbia avuto modo di consultare l'informativa in ordine al trattamento dei dati che lo riguardano, se l'informativa sia sufficientemente granulare e specifica e se sia stato effettivamente prestato un consenso pieno e consapevole in ordine all'utilizzo che dei propri dati ne possa fare non solo l'*infomediario*, ma anche i soggetti che, tramite l'intermediario, andranno a beneficiare di tali dati personali.

Invero, dubbi sorgono proprio sulla possibilità di delegare a soggetti terzi, tra l'altro operatori commerciali, atti di esercizio di diritti che attengono non alla sfera patrimoniale, ma a quella strettamente personale, in ragione delle ineliminabili esigenze di salvaguardia dei diritti della personalità in cui rientra il diritto alla protezione dei dati personali. Anche qualora tale delega si ritenesse ammissibile sotto il profilo giuridico, sarebbe quanto mai opportuno che, proprio in funzione della esigenze di protezione dei diritti della personalità, incontrasse rigorosi limiti, che possono essere eventualmente estrapolati dall'ordinamento giuridico anche operando a livello interpretativo sui principi generali, (ragionando ad esempio sul principio di liceità e correttezza, quello di minimizzazione e quello di finalità), unitamente ai requisiti richiesti per il consenso al trattamento, che potrebbero assistere – *mutatis mutandis* – anche le ulteriori manifestazioni di volontà rese dall'interessato con riguardo alla fattispecie di trattamento a lui relative, con particolare riferimento alla delega.

La commercializzazione dei dati mediante *infomediari* può essere percorsa anche attraverso modelli di *business* diversi, in cui il mediatore operante nel mercato delle informazioni eserciti il pro-

prio ruolo senza accentrare su di sé i dati degli interessati e senza essere destinatario di deleghe con i soggetti terzi.

Si consideri ad esempio il caso in cui l'intermediario dei dati si proponga di agire come soggetto che "gestisce la *privacy*" per l'interessato (ad es. come «*Privacy Knowledge Manager», quale dichiara di essere ErnieApp nella fornitura del proprio servizio: v., supra*), allestendo un'interfaccia che consenta all'interessato medesimo, via *web* o via *app*, di operare in autonomia sulle impostazioni rilevanti in materia di protezione dei dati personali (c.d. "*privacy setting*") predisposte dai diversi *providers*, che mirano a utilizzare i dati per finalità commerciali o di altra natura. Qui occorre considerare che, pur venendo meno le questioni in ordine alla portabilità dei dati e – a quanto parrebbe – della delega, rimangono pur sempre le altre questioni relative alla gestione dell'eventuale sussistenza del conflitto di interessi dell'*infomediario*, nonché quelle concernenti la corretta manifestazione del consenso (e degli altri parametri rilevanti in materia di protezione dei dati personali) gestiti mediante il sistema informatico dell'*infomediario* medesimo, a seguito di accordi (di commercializzazione) intercorsi con i *providers* interessati all'utilizzo dei dati personali, per proprie finalità.

Andrebbe cioè verificato di volta in volta se siano quantomeno rispettati i requisiti del consenso (che deve essere pieno, informato, specifico, inequivoco e libero, anche con riguardo alla c.d. "granularità") e dunque se, in relazione agli specifici servizi per i quali i destinatari finali delle informazioni ottengono il consenso al trattamento dei dati personali dell'interessato, sia stata fornita un'adeguata informativa tramite il sistema tecnologico approntato dall'*infomediario*. Andrebbero inoltre verificati, oltre ai presupposti giuridici che assicurano la liceità e la correttezza del trattamento con riguardo agli altri parametri che il sistema consente di gestire con i "*privacy setting*" (ad es., la completezza dell'informativa e le corrette modalità di gestione del consenso per l'utilizzo dei *cookies* o per le impostazioni di geolocalizzazione), se siano rispettati anche i principi generali in materia di protezione dei dati personali, incluso il principio di finalità, minimizzazione, etc., da verificare non solo nei confronti dell'infomediario, ma anche dei singoli *providers* messi in relazione con gli interessati attraverso il servizio *de quo*. Si tratta di un'indagine che ovviamente non può prescindere

da una valutazione caso per caso e che non può essere condotta in questa sede, esulando dagli obiettivi del presente lavoro.

Rimane da considerare la facoltà, per l'interessato, di richiedere somme di denaro per l'utilizzo dei dati personali, quali attributi della propria personalità (a cui rifugge la qualificazione di merce): nel sito Internet in cui viene illustrato il servizio ErnieApp, infatti, viene dato particolare risalto a quello che viene enfaticamente denominato «*The Right to Monetize* (RTM)*», definito dall'infomediario come «a new public policy notion which we conceptualised and which we propose to become an integral part of consumer digital rights. Under RTM we seek to change the paradigm that governs users and companies' relationship on the internet whereby companies never pay users for the data they generate and in exchange they enjoy free services. With RTM we want to introduce a general fairness principle under which users who contribute with data to companies' profitability should be receiving a fair, non-discriminatory, proportionate gain as key "partners" and/or "suppliers" in the rich ecosystem of the digital economy. The compensation is conceived to reward the persistent willingness of the user to continue share data which are used by the internet company to make a profitable business and when this company wants to use/share the data with other 3rd parties (pass through the user consent). In practice RTM would make very transparent and accountable for companies to use people's data. The system would reward those companies that commit to be privacy transparent and accountable toward end-users. The scheme would apply to all users generated data, including those data that get anonymized by companies for further usage*»[84].

Invero, l'ordinamento già riconosce da tempo la possibilità per l'interessato di ottenere un compenso per l'utilizzo di attribuiti della persona, come avviene ad esempio per l'utilizzo dell'immagine a fini commerciali o per gli sconti (o altri premi) ottenuti per il trattamento dei dati personali in occasione dell'utilizzo di *fidelity card*. L'innovazione, dunque, non è nel diritto ad ottenere un corrispettivo in denaro a fronte dell'utilizzo dei dati personali oggetto

[84] Cfr. le pagine del sito Internet di illustrazione del servizio ErnieApp, all'indirizzo https://ernieapp.com.

di commercializzazione, ma, semmai, nell'avvento di nuovi modelli di *business* concernenti i dati personali, che – dando corpo al "diritto" a trattare dati personali nello svolgimento dell'attività economica[85] – lascia spazio a nuovi ruoli nel mercato dell'*infomediation*, attualmente pressoché inesplorato sotto il profilo giuridico, ma destinato ad imporsi all'attenzione dell'interprete, delle *Authorities* e del legislatore, nella prospettiva costante del bilanciamento tra tutela della persona ed esigenze del mercato[86].

4. I servizi di condivisione dei dati nella proposta di regolamento sulla *governance* europea dei dati (*Data Governance Act*)

4.1. *Servizi di* data sharing *e ruolo degli intermediari di dati al cospetto del mercato*

Nell'ambito delle predette dinamiche di mercato e con l'intento di avvalorare le potenzialità offerte dalla commercializzazione dei dati personali, il legislatore europeo sembra abbia voluto fornire una significativa riposta alle predette questioni giuridiche, con la proposta di regolamento del 25 novembre 2020 in materia di *European Data Governance* [COM(2020) 767 final], nel quale viene delineata, tra l'altro, la disciplina di alcuni aspetti concernenti la fornitura del «*servizio di condivisione dei dati» (inclusi quelli personali), intesa come «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» (art. 2, par. 1, n. 7, della proposta di regolamento sulla governance* europea dei dati).

---

[85] V., *amplius*, Bravo, *Il diritto a trattare dati personali nello svolgimento dell'attività economica*, cit., *passim*.

[86] Su tale bilanciamento si veda, più diffusamente, Zorzi Galgano, *Le due anime del GDPR e la tutela del diritto alla privacy*, cit., p. 35 ss.; nonché Bravo, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, in *Contratto e impresa*, 2018, n. 1, pp. 190 ss.

Quello dell'intermediazione dei dati è settore ancora non armonizzato a livello europeo e la necessità di intervenire in tempi rapidi hanno imposto la scelta del regolamento: non sconta tempi di recepimento nel diritto interno, in quanto non occorrono atti normativi di attuazione nei singoli ordinamenti nazionali e, inoltre, introduce norme immediatamente applicabili, in maniera uniforme, in tutta l'UE.

La disciplina è contenuta nel Capo III, il quale, come si legge nella relazione introduttiva, «mira ad accrescere la fiducia nella condivisione dei dati personali e non personali, come pure a ridurre i costi di transazione relativi alle condizioni dei dati tra imprese (B2B) e da consumatore a impresa (C2B) grazie alla creazione di un regime di notifica per i fornitori di servizi di condivisione dei dati. Tali fornitori dovranno soddisfare una serie di requisiti, in particolare quello di rimanere *neutrali* in merito ai dati scambiati. Non possono utilizzare tali dati per altri scopi. Nel caso dei fornitori di servizi di condivisione dei dati che offrono i loro servizi a persone fisiche dovrà inoltre essere soddisfatto il criterio aggiuntivo di assunzione degli obblighi fiduciari nei confronti di chi li utilizza. L'approccio è volto a garantire un funzionamento aperto e collaborativo dei servizi di condivisione dei dati e a rafforzare il ruolo delle persone fisiche e giuridiche offrendo loro una migliore panoramica dei loro dati e un maggiore controllo sugli stessi. Un'autorità competente designata dagli Stati membri sarà responsabile del monitoraggio della conformità ai requisiti connessi alla fornitura di tali servizi».

Sin dalla lettura dei *considerando* emerge chiaramente il ruolo degli infomediari nelle nuove strategie dell'UE. Così, «Si prevede che i fornitori di servizi di condivisione dei dati (intermediari di dati) svolgano un ruolo essenziale nell'economia dei dati, operando in qualità di strumenti che agevolano l'aggregazione e lo scambio di quantità considerevoli di dati pertinenti. Gli intermediari di dati che offrono servizi che collegano i diversi soggetti dispongono del potenziale per contribuire alla messa in comune efficiente dei dati come pure all'agevolazione della condivisione bilaterale dei dati. Gli intermediari di dati specializzati, che sono indipendenti tanto dai titolari dei dati quanto dagli utenti dei dati, possono facilitare l'emergere di ecosistemi basati sui dati indipendenti da qualsiasi

operatore che detenga un grado significativo di potere di mercato (…)»[87].

L'attenzione per le dinamiche commerciali sui dati è altresì rimarcata là dove si afferma che, sempre con riguardo all'infomediazione, la disciplina delineata nella proposta di regolamento sulla *data governance* «dovrebbe contemplare solo i fornitori di servizi di condivisione dei dati il cui obiettivo principale è la creazione di un rapporto commerciale, giuridico e potenzialmente anche tecnico tra i titolari dei dati, compresi gli interessati, da un lato, e i potenziali utenti, dall'altro, e la prestazione di assistenza a entrambe le parti nelle transazioni reciproche di *asset* di dati (…)»[88].

La proposta normativa, dunque, guarda ai servizi di intermediazione dei dati non già come ad una minaccia per i diritti fondamentali dell'interessato – segnalata dal nostro Garante per la protezione dei dati personali a livello europeo dopo la prima disamina del caso Weople, sopra discusso – quanto invece come un'opportunità per il mercato, non più da lasciare a se stesso, però, ma da "governare" in maniera più stringente, tramite un puntuale sistema di sorveglianza, su cui si tornerà a breve.

4.2. *«Titolare dei dati» e «utente dei dati»*

Gli *infomediari* assicurano la creazione del mercato dei dati, funzionale all'economia ed allo sviluppo di una *data-driven society* e, in tali logiche, gli interessati al trattamento dei dati personali vengono ora visti come «*titolari dei dati», che, tramite intermediari, colgono le opportunità del mercato concedendone l'accesso e l'utilizzo nei confronti di altri soggetti, gli «utenti dei dati».*

Il «*titolare dei dati» (data holder*), per la nuova proposta di regolamento, è «la persona giuridica o l'interessato che, conformemente al diritto dell'Unione o nazionale applicabile, ha il diritto di concedere l'accesso a determinati dati personali o non personali sotto il proprio controllo o di condividerli» (art. 2, par. 1, n. 5, della proposta cit.). Il mutamento del lessico, some già evidenziato

[87] *Considerando* n. 22, prop. di reg. cit.
[88] *Ibidem*.

supra, è indice di un cambio di paradigma nell'approccio del legislatore, perché tende ad oggettivare i dati personali in funzione del loro impiego economico, con il serio rischio di una progressiva perdita di tutela per gli attributi della persona e, con essa, per i diritti della personalità.

La condivisione dei dati consente infatti all'interessato, neonominato «titolare dei dati», di concederne l'accesso o l'utilizzo all'«utente dei dati» (*data user*), ossia alla «persona fisica o giuridica che ha *accesso legittimo* a determinati dati personali o non personali ed è *autorizzata* a utilizzare tali dati a fini commerciali o non commerciali» (art. 2, par. 1, n. 6, della proposta cit.). Se usassimo il lessico del GDPR con riguardo ai dati personali, l'«utente dei dati» personali altri non è che il titolare del trattamento.

Si noti che non viene introdotta solo una novità prettamente terminologica: si usano concetti che spostano l'attenzione sulla commercializzazione dei dati personali, spingendo verso una reificazione dei dati al fine di favorire la creazione di mercati alternativi rispetto a quelli creati dai *Big Tech*.

La «titolarità» del dato, almeno con riguardo a quelli di carattere personale, non deve però essere collocata sul piano del diritto dominicale o dei diritti di proprietà intellettuale: è piuttosto da inquadrate sul piano dei diritti della personalità. I dati personali, anche di fronte alle nuove norme, sono pur sempre attributi della persona, nei cui confronti l'ordinamento europeo esplicita alcune delle facoltà di disposizione da parte dell'interessato, a cui i dati appartengono (*data holder*): questi può concedere a terzi l'*accesso* a tali dati o la fruizione in *condivisione*, finanche l'utilizzo per finalità commerciali, ma sempre «sotto il proprio controllo». La dimensione del «*controllo*», menzionata espressamente nella *definizione di titolare dei dati*, perdura anche di fronte alla concessione dell'accesso o della condivisione in favore dell'utente dei dati, per l'utilizzo commerciale o non commerciale che questi ne faccia e ciò, con riguardo ai dati personali, è funzionale alla loro natura di attributo della persona, non disponibile e non rinunciabile ed è ricollegabile al concetto di *autodeterminazione informativa* ben esplorato in dottrina. Quella che fa capo al titolare dei dati, ove essi abbiano natura di dati personali, è dunque una situazione giuridica soggettiva attiva che, in linea con la ricostruzione dottrinale e giuri-

sprudenziale maturata con riguardo alle norme in materia di protezione dei dati personali, è riconducibile ai diritti della personalità e, quindi, a quei diritti solo "trovati" dall'ordinamento giuridico, per usare un'efficace espressione di Francesco Galgano[89]. Nell'affermare il diritto del «titolare dei dati» di concedere l'accesso o la condivisione in favore di altri (gli «utenti di dati»), il *Data Governance Act* pone l'accento anche su altre situazioni giuridiche: quelle dei *data users* che vantano proprie situazioni giuridiche soggettive attive, variamente qualificabili, a seconda di come si atteggia concretamente la fattispecie di trattamento[90] e, dunque, difficilmente definibili a priori: ove l'autorizzazione all'accesso venga a configurarsi come rimozione di un limite previsto dall'ordinamento quale tecnica di bilanciamento degli interessi giuridicamente rilevanti e quale meccanismo di controllo della liceità del trattamento, l'attività di trattamento verrebbe a configurarsi in capo al titolare del trattamento (*data user*) in forza di poteri o diritti di cui è già titolare *ex ante*, riconducibili o a poteri di natura giuspubblicistica (es., i poteri autoritativi degli enti pubblici, esercitabili in funzione del perseguimento di interessi pubblici) o a diritti fondamentali (come ad es. il diritto di libera manifestazione del pensiero o il diritto di esercitare liberamente l'attività economica)[91]; non è da escludere che, soprattutto a seguito delle nuove disposizioni normative contenute nel *Data Governance Act*, la fattispecie concreta possa far configurare attribuzioni di facoltà nell'utilizzo dei dati secondo le logiche del diritto di natura obbligatoria, accostabile alla concessione delle licenze d'uso[92]. Su tali aspetti si imporrebbero appro-

---

[89] Galgano, *Trattato di diritto civile*, I, 3ª ed. a cura di Zorzi Galgano, 2014, p. 171,

[90] Sulla fattispecie di trattamento v. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., p. 42 ss.

[91] Sulla qualificazione del diritto dell'utente di dati personali, quale titolare del trattamento di dati personali, si rinvia a Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., *passim*, e, ivi, spec. p. 57 ss. Le novità che si affacciano con le nuove norme dell'*European Data Governance* sollecitano nuove direzioni di ricerca che richiedono un autonomo approfondimento.

[92] In questo senso si veda Alvisi, *Dati personali e diritti dei consumatori*,

fondimenti di ricerca che, per esigenze di economia del discorso, si demandano ad altra sede.

4.3. *Caratteristiche, confini e funzioni del servizio di* data sharing

Il servizio di condivisione dei dati, tuttavia, ha confini da precisare: nella proposta citata si afferma che la disciplina sarebbe rivolta soltanto ai «servizi che mirano a garantire un'intermediazione tra un numero indefinito di titolari e un numero indefinito [di] utenti dei dati, a esclusione dei servizi di condivisione dei dati destinati a essere utilizzati da un gruppo chiuso di titolari e utenti dei dati»[93]. Ancora, «Dovrebbero essere esclusi i fornitori di servizi *cloud*, nonché i fornitori di servizi che ottengono dati dai titolari dei dati, li aggregano, arricchiscono o trasformano e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza stabilire un rapporto diretto tra i titolari dei dati e gli utenti dei dati, ad esempio intermediari pubblicitari o di dati, consulenti di dati, fornitori di prodotti di dai risultanti dal valore aggiunto ai dati dal fornitore del servizio»[94].

Non sembra applicabile la disciplina neanche ai servizi di *social network*, né alle piattaforme IOT (I*nternet of Things*) volte ad utilizzare i dati generati da oggetti interconnessi, se si pensa che – in base alla lettura dei *considerando* – la disciplina delineata nella proposta di regolamento «non dovrebbe contemplare le piattaforme di scambio dei dati utilizzate esclusivamente dai titolari di dati per consentire l'utilizzo dei dati da essi detenuti, come pure le piattaforme sviluppate nel contesto di oggetti e dispostivi con-

---

in *I dati personali nel diritto europeo*, a cura di Cuffaro, D'Orazio e Ricciuto, cit., p. 675, ove fa riferimento ad «accordi in virtù dei quali i consumatori fruiscono, apparentemente a titolo gratuito, di servizi digitali (di *social networking*, di comunicazione vocale tramite protocollo internet, di messaggistica online, ecc.) in cambio di una *licenza d'uso* pressoché illimitata *dei loro dati personali*, di regola non tecnicamente necessaria per la fornitura del servizio digitale di cui costituisce remunerazione».

[93] *Considerando* n. 22, prop. di reg. cit.

[94] *Ibidem*.

nessi all'Internet delle cose il cui principale obiettivo è garantire funzionalità dell'oggetto o dispositivo connesso e rendere possibili servizi a valore aggiunto (…)»[95].

Vero è che il servizio di condivisione dei dati può riferirsi sia a dati personali che a dati non personali, ma l'intenzione che anima il legislatore europeo nella nuova proposta sulla *data governance* è chiara: l'intermediazione sui dati tra il «titolare dei dati» (interessato) e l'«utente dei dati» (titolare del trattamento), per l'instaurazione di un rapporto giuridico e commerciale sui dati medesimi, viene perseguita in maniera decisa soprattutto con riguardo ai dati di natura personale. A tal riguardo il *considerando* n. 23 chiarisce che «Una categoria specifica di intermediari di dati comprende i fornitori di servizi di condivisione dei dati che offrono i loro servizi agli interessati ai sensi del regolamento (UE) 2016/679. *Tali 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 li riguardano (…)»[96].

Vengono ripercorse, in tale *considerando*, le caratteristiche e le funzioni del servizio di *infomediazione*: «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 (…)»[97].

4.4. *Servizi di condivisione dei dati e tutela degli interessati. Conflitti di interesse e «incentivi disallineati»*

Con riguardo ai dati personali, dunque, gli intermediari gestiscono per conto degli interessati del trattamento (definiti «titolari dei dati») tutti i diritti degli interessati che il GDPR accorda loro,

---

[95] *Ibidem*.
[96] *Considerando* n. 23, prop. di reg. cit.
[97] *Ibidem*.

incluso il diritto al consenso e il diritto alla portabilità dei dati, in linea con i modelli di business già riscontrati nella prassi e sui quali s'è destata la preoccupazione del nostro Garante per la protezione dei dati personali. Sorgono dunque problemi legati alla tutela dell'interessato contro i rischi di abuso da parte degli *infomediari*.

La nuova proposta di regolamento chiarisce, a tal riguardo, che nel contesto sopra delineato «è importante che il loro modello commerciale garantisca che non vi siano *incentivi disallineati* che incoraggino i singoli individui a mettere a disposizione più dati di quanto non sia nel loro stesso interesse. Ciò potrebbe comprendere l'offerta di consulenza ai singoli individui quanto agli utilizzi dei loro dati cui potrebbero acconsentire e il controllo della dovuta diligenza degli utenti dei dati prima che sia consentito loro di contattare gli interessati, al fine di evitare pratiche fraudolente. In alcune situazioni potrebbe essere auspicabile raccogliere dati reali in uno spazio di conservazione dei dati personali o "spazio di dati personali", affinché il trattamento possa aver luogo all'interno di tale spazio senza che i dati personali siano trasmessi a terzi, al fine di ottimizzare la protezione dei dati personali e della *privacy*»[98].

4.5. (segue) *Gestione dei diritti dell'interessato e delega*

C'è da chiedersi se, al cospetto delle nuove norme, l'intermediario dei dati personali, nel "gestire" i diritti dell'interessato per conto dell'interessato medesimo, possa essere destinatario di una delega in tal senso, che lo legittimi ad agire in nome e per conto del «*titolare dei dati*». *La questione della possibilità o meno di conferire delega ad un infomediario*, anche al fine di gestire il consenso al trattamento e la portabilità dei dati per conto dell'interessato medesimo nei confronti di fornitori terzi s'è posta nell'indagine avviata dal Garante per il caso Weople, sora analizzato. Nella proposta di direttiva sulla *European Data Governance* mi sembra che la scelta sia nel senso di ammettere la possibilità della delega in tale contesto, ma con una limitazione data dall'obbligo di neutralità dell'intermediario. La delega non solo appare insita nella facoltà,

[98] *Ibidem*.

da parte dell'*infomediario*, di gestire il consenso e gli altri diritti dell'interessato, ma si desume anche – *a contrario* – dal *considerando* n. 24 in materia di «cooperative di dati», che «mirano a rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati [ossia dalle organizzazioni di titolari dei dati personali, *n.d.a.*], cui è subordinato l'utilizzo dei dati o risolvendo potenziali controversie tra membri di un gruppo sulle modalità di utilizzo dei dati quanto tali dati riguardano più interessati all'interno di tale gruppo. In tale contesto è importante riconoscere che i diritti a norma del regolamento (UE) 2016/679 possono essere esercitati soltanto a titolo individuale e *non possono essere conferiti o delegati* a una cooperativa di dati (…)»[99].

La logica dell'esclusione non risiede in un'ipotetica natura personalissima del diritto da far valere, che ne impedirebbe l'esercizio per delega da parte di altri soggetti: basti pensare che il GDPR afferma, per il consenso al trattamento di dati personali relativi a minori, i casi in cui questo debba essere fornito non dal minore medesimo, in proprio, ma dai suoi genitori, a riprova che non è considerato atto personalissimo. La delega da parte dell'interessato ad altro soggetto per l'esercizio del diritto sembra qui ammessa con il limite tuttavia del divieto di una gestione "collettiva" ed "aggregata". Di qui l'impossibilità di delega verso la sola cooperativa di dati, senza alcuna preclusione, invece, per il conferimento della delega all'intermediario dei dati, per l'esercizio a titolo individuale dei diritti riconosciuti dal GDPR.

4.6. (segue) *Finalità esclusiva, neutralità, separazione strutturale nella fornitura dei servizi, entità giuridica distinta*

Per arginare rischi di abusi da parte dell'*infomediario*, che sarebbero drasticamente lesivi non solo dei diritti fondamentali dell'interessato, ma – nella prospettiva del legislatore europeo – soprattutto di quella fiducia considerata necessaria per la realizza-

[99] *Considerando* n. 24, prop. di reg. cit.

zione del mercato dei dati, occorre che all'intermediario sia preclusa la facoltà di utilizzare i dati per fini diversi ed ulteriori da quelli concernenti il servizio di condivisione dei dati. Così il *considerando* n. 26 rimarca che «Un elemento essenziale per infondere fiducia e garantire maggiore controllo ai titolari e agli utenti dei dati nei servizi di condivisione dei dati è la *neutralità* dei fornitori del servizio di condivisione dei dati riguardo ai dati scambiati tra titolari e utenti dei dati. È pertanto necessario che i fornitori di servizi di condivisione dei dati agiscano solo in qualità di intermediari nelle transazioni e non utilizzino per *nessun altro fine* i dati scambiati (…)»[100]. La riferita neutralità comporta una necessaria «*separazione strutturale* tra il servizio di condivisione dei dati e qualsiasi altro servizio fornito, in modo tale da evitare problemi di conflitto di interessi. Ciò significa che il servizio di condivisione dei dati dovrebbe essere fornito mediante un'*entità giuridica distinta* dalle altre attività di tale fornitore di servizio di condivisione dei dati. I fornitori di servizi di condivisione dei dati che agiscono da intermediari tra i singoli individui, quali i titolari dei dati, e le persone giuridiche dovrebbero inoltre avere l'obbligo fiduciario nei confronti dei singoli individui di garantire che agiscono nel migliore interesse dei titolari dei dati»[101].

4.7. Obbligo di notifica e sistema di vigilanza

La disciplina che si vuole dettare in materia di servizi di condivisione dei dati introduce poi un obbligo di notifica, da parte dell'intermediario (fornitore del servizio di condivisione) ad un'autorità di controllo competente, senza far venir meno il concomitante controllo da parte di autorità competenti in altri settori, come in materia di concorrenza e in materia di trattamento di dati personali[102]. La notifica è preventiva rispetto allo svolgimento dell'attività, autorizza il fornitore allo svolgimento dei servizi in tutti gli Stati membri dell'UE e deve contenere le seguenti informazioni:

---

[100] *Considerando* n. 26, prop. di reg. cit.
[101] *Ibidem*.
[102] Cfr. art. 9, par. 1 e 2, e art. 10, prop. di reg. cit.

a) identità del fornitore di servizi di condivisione dei dati; *b) status* giuridico, forma giuridica e numero di registrazione nel registro delle imprese o altro pubblico registro analogo; *c)* indirizzo dello stabilimento principale o di eventuali sedi secondarie; *d)* il sito *web* in cui sono reperibili le informazioni sul fornitore e la sua attività; *e)* le persone di contatto e i recapiti del fornitore: *f)* una descrizione del servizio che il fornitore intende fornire; *g)* la data prevista di inizio attività; *h)* gli Stati membri in cui il fornitore intende fornire i servizi[103].

Ricevuta la notifica, l'autorità competente di uno Stato membro è tenuta a trasmettere la notifica alle altre autorità competenti degli altri Stati membri, nonché alla Commissione europea, che tiene un registro dei fornitori dei servizi di condivisione dei dati[104]. La notifica è dovuta dal fornitore anche in caso di cessazione dell'attività.

Le autorità competenti, destinatarie delle notifiche, svolgono compiti di vigilanza e controllo sull'attività dei fornitori dei servizi di condivisione dei dati e, per lo svolgimento di tale attività, possono imporre tariffe proporzionali e oggettive, basate sui costi amministrativi relativi al monitoraggio della conformità al Capo III dell'emanando regolamento sulla *data governance* – dedicato ai servizi di condivisione dei dati – e ad altre attività di controllo del mercato, sempre correlate alle notifiche dei servizi di condivisione dei dati[105].

I poteri dell'autorità di controllo sono molto ampi: ha funzioni di vigilanza sul servizio di condivisione dei dati, monitorando e controllando la *compliance* con il regolamento sulla *data governance*; può richiedere ai fornitori dei servizi di condivisione dei dati tutte le informazioni necessarie alla verifica della conformità, soprattutto con riguardo ai requisiti e alle condizioni per la fornitura del servizio ed, in caso di violazione – a seguito di accertamento con un procedimento nell'ambito del quale al fornitore deve essere accordata la facoltà di esprimere osservazioni entro un tempo

[103] Cfr. art. 10, prop. di reg. cit.
[104] *Ibidem*.
[105] *Ibidem*.

ragionevole – possono adottare misure adeguate e proporzionali per garantire la conformità al regolamento sulla *data governance* e, ove ritenuto opportuno, possono anche imporre sanzioni pecuniarie dissuasive (incluso *sanzioni periodiche* con *effetto retroattivo*) e chiedere la cessazione o il rinvio della fornitura del servizio di condivisione dei dati (art. 13).

4.8. (segue) *Condizioni per la fornitura del servizio*

La pervasività del controllo si apprezza analizzando le «*condizioni* per la fornitura di servizi di condivisione dei dati», previste all'art. 11, su cui l'autorità competente di ogni Stato membro è tenuta ad effettuare l'attività di vigilanza.

La prima "condizione" riguarda il principio di *neutralità*, sopra richiamato, che trova la sua applicazione nell'*esclusività dello scopo* per cui il trattamento viene posto in essere e per il criterio di *separazione*, sotto il profilo soggettivo, tra chi fornisce il servizio di condivisione dei dati e chi tali dati li utilizza: il fornitore, intermediario dei dati, non può utilizzare i dati oggetto del servizio di condivisione – siano essi dati personali o non personali – per scopi diversi dalla messa a disposizione di dati agli "utenti dei dati" «e i servizi di condivisione dei dati rientrano in un'entità giuridica distinta»[106]. Si sarebbe potuto fare sicuramente di più: è facile prevedere che la distinzione soggettiva tra chi fornisce i dati in condivisione e chi li utilizza venga rispettato solo formalmente, ad esempio, attribuendo ad una società, appartenente al medesimo gruppo societario di quelle che poi utilizzeranno i dati, le funzioni di *data sharing* in favore (anche) delle altre società appartenenti al medesimo gruppo. Sarebbe stato preferibile ampliare il criterio, allargandolo anche ai gruppi societari, ovvero a società controllate o collegate. L'impatto è sia sulle dinamiche concorrenziali, sia sulle effettive esigenze di tutela degli interessati di fronte a condotte prevaricatorie, a cui la logica della commercializzazione dei dati personali, che rimangono pur sempre "attributi della personalità", potrebbe spingere.

[106] Art. 11, par. 1, n. 1, prop. di reg. cit.

Su questo fronte le autorità di vigilanza possono comunque esercitare la loro azione: per un verso rimane sempre ferma la tutela offerta dal GDPR, che consentirebbe alle autorità di controllo in materia di protezione dei dati personali di intervenire, anche d'ufficio, ove ravvisassero un *vulnus* ai diritti dell'interessato; per altro verso, rimanendo nell'ambito delle norme sulla *data governance*, la competente autorità di controllo può far leva su altre "condizioni" per la fornitura del servizio di *data sharing*.

Ai sensi dell'art. 11 cit., infatti, il fornitore deve predisporre ed adottare procedure atte a garantire il rispetto della disciplina europea e nazionale in materia di concorrenza[107] e deve provvedere «affinché la procedura di accesso al suo servizio sia equa, trasparente e non discriminatoria sia per i titolari dei dati sia per gli utenti dei dati, anche per quanto riguarda i prezzi»[108].

Quanto invece alla tutela del "titolare dei dati", (i) viene allargato anche ai «*metadati*» l'esclusività dello scopo, legato necessariamente alla fornitura del servizio di *data sharing*[109], (ii) viene vincolata la fornitura del servizio agli interessati al perseguimento dell'«interesse superiore di questi ultimi nel facilitare l'esercizio dei loro diritti, in particolare fornendo loro consulenza sui potenziali utilizzi dei dati e sui termini e le condizioni standard collegati a tali utilizzi»[110] e (iii) viene imposto l'obbligo di adottare «procedure per prevenire pratiche fraudolente o abusive in relazione all'ac-

[107] Art. 11, par. 1, n. 9, prop. di reg. cit.

[108] Art. 11, par. 1, n. 3, prop. di reg. cit.

[109] Art. 11, par. 1, n. 2, prop. di reg. cit., ai sensi del quale «i metadati raccolti nel corso della fornitura del servizio di condivisione dei dati possono essere utilizzati solo per lo sviluppo di tale servizio».

[110] Art. 11, par. 1, n. 10, prop. di reg. cit. Rispetto alle più altisonanti intenzioni declamate nei considerando, che indirizzavano la consulenza anche sul fronte della tutela dei diritti dell'interessato, in particolare quelle accordate dalla disciplina in materia di protezione dei dati personali, qui la disposizione pare fermarsi sul piano delle dinamiche commerciali e contrattuali, nella prospettiva di incentivarne sia lo sfruttamento patrimoniale, sia le possibilità stesse di utilizzo nei diversi contesti sociali ed economici, funzionali all'ingresso dei dati nel mercato che il *data sharing* intende favorire.

cesso ai dati da parte di soggetti che richiedono l'accesso tramite i suoi servizi»[111], che sarebbe utile ricollegare con la disciplina sulla responsabilità amministrativa degli enti di cui al d.lgs. n. 231 del 2001.

A maggior garanzia del "titolare dei diritti" si prevede poi che il fornitore metta in atto adeguate misure non solo «tecniche» e «organizzative», ma anche «giuridiche», «al fine di impedire il trasferimento di dati non personali o l'accesso a questi ultimi nel caso in cui ciò sia illegale a norma del diritto dell'Unione»[112]. Si noti però, qui, una restrizione drastica dell'ambito di applicazione della norma, che non si estende ai "dati personali" e tale scelta di riflette anche in altra "condizione" per la fornitura del servizio di *data sharing*, che impone l'adozione di «misure per garantire un elevato livello di sicurezza per la conservazione e la trasmissione di *dati non personali*»[113]. La *ratio* di tali esclusioni sembra ravvisabile nell'esistenza di obblighi analoghi previsti dalla disciplina in materia di protezione di dati personali, già presidiati da un sistema di vigilanza (affidato alle autorità di controllo in materia di protezione dei dati personali) che esercitano poteri anche inibitori e sanzionatori a presidio dei diritti dell'interessato. A tal riguardo va infatti ricordato che il fornitore del servizio di condivisione dei dati, qualora detto servizio abbia ad oggetto dati personali, è egli stesso "titolare del trattamento dei dati personali", ancorché per le finalità di *data sharing*, sicché è comunque tenuto, ai sensi del Reg. UE n. 679/2016, all'adozione delle misure tecniche e organizzative (incluse quelle "giuridiche") ivi contemplate e, segnatamente, (i) quelle in tema di *data protection by design* e *by default* (art. 25 GDPR), (ii) quelle in tema di prevenzione dai rischi di violazione dei dati (art. 32 GDPR), (iii) quelle in tema di *accountability*, per garantire e per dimostrare la *compliance* al GDPR (art. 24 GDPR).

È invece applicabile sia ai dati personali che ai dati non personali l'obbligo per il fornitore di garantire la *business continuity*

[111] Art. 11, par. 1, n. 5, prop. di reg. cit.
[112] Art. 11, par. 1, n. 7, prop. di reg. cit.
[113] Art. 11, par. 1, n. 8, prop. di reg. cit.

del servizio di *data sharing*[114], con la precisazione che, ove tale servizio garantisca anche la conservazione dei dati, il fornitore è tenuto altresì a di disporre «di garanzie sufficienti che consentano ai titolari dei dati e agli utenti dei dati di ottenere l'*accesso* ai loro dati in caso di insolvenza»[115]. Per la verità i diritti di accesso ai dati personali oggetto di conservazione da parte di un titolare del trattamento sono contemplati anche nell'art. 15 GDPR, ma ciò non ha impedito, nel *Data Governance Act*, una previsione *ad hoc* con riguardo al servizio di condivisione di dati, nell'ambito del quale l'accesso è facoltà assicurata sia al "titolare dei dati" (interessato al trattamento, ove la condivisione abbia ad oggetto dati personali), sia all' "utente dei dati" (titolare del trattamento che utilizzi i dati personali oggetto di condivisione per scopi commerciali o non commerciali).

Altra "condizione" per la fornitura del servizio di condivisione dei dati, in particolare qualora abbia ad oggetto dati personali, si colloca in una prospettiva di ideale continuità con il diritto alla portabilità dei dati di cui all'art. 20 GDPR. La proposta di regolamento sulla *data governance* prevede infatti l'ulteriore obbligo, per il fornitore dei servizio di *data sharing*, di «agevolare lo scambio dei dati nel formato in cui li riceve dal titolare dei dati e li converte in formati specifici solo allo scopo di migliorare l'interoperabilità a livello intrasettoriale e intersettoriale, se richiesto dall'utente dei dati, se richiesto dal diritto dell'Unione o per garantire l'armonizzazione con le norme internazionali o europee in materia di dati»[116]. Uno dei problemi applicativi della *data portability* risiede proprio nella compatibilità tra formati di dati utilizzati dal titolare del trattamento tenuto alla trasmissione dei dati e quelli utilizzati dal titolare del trattamento destinatario della trasmissione dei dati, a richiesta dell'interessato, in formato elettronico, strutturato e leggibile da dispositivo. Medesimo problema può ovviamente riscontrarsi per la condivisione di dati non personali, sicché il sistema delineato dall'emanando regolamento sulla data *governance*

[114] Art. 11, par. 1, n. 6, prop. di reg. cit.
[115] *Ibidem*.
[116] Art. 11, par. 1, n. 4, prop. di reg. cit.

fa leva proprio sugli *infomediari* per risolvere anche i problemi tecnici di interoperabilità, in un'offerta a valore aggiunto che, per un verso, mette in contatto "domanda" e "offerta" di dati e, per altro verso, la favorisce e l'amplifica, con attività di consulenza e con interventi di natura tecnica.

Un'ultima "condizione" prevede poi che «qualora fornisca strumenti per ottenere il consenso degli *interessati* o le autorizzazioni a trattare i dati messi a disposizione da persone giuridiche, il fornitore specifica la giurisdizione o le giurisdizioni in cui si intende effettuare l'utilizzo dei dati»[117]. Vanno considerate incluse negli obblighi informativi ora in esame anche le indicazioni sull'ambito di applicazione materiale e territoriale di cui agli artt. 2 e 3 del GDPR, per i trattamenti di dai personali.

Nelle "condizioni" per la fornitura del servizio mancano, invece, norme *ad hoc* sulla prevenzione e sulla gestione del "conflitto di interessi" tra fornitore del servizio di *data sharing* e utenti (fruitori anche per scopi commerciali) dei dati. L'inserimento di una "condizione" che ne facesse espressamente menzione sarebbe stata opportuna, in quanto avrebbe allargato di molto, in tale direzione, i poteri dell'autorità di vigilanza e avrebbe offerto maggiori garanzie nel contrastare i rischi di abuso nei confronti degli interessati, oltre che nelle dinamiche concorrenziali. Mi pare tuttavia che, anche senza tale specifica "condizione", quelle delineate nel *Data Governance Act* offrano comunque ampi poteri di intervento all'autorità di vigilanza, su molteplici fronti.

4.9. *Sull'individuazione dell'autorità di vigilanza competente*

C'è da chiedersi quale sia l'autorità più indicata per lo svolgimento delle funzioni di vigilanza *in subjecta materia*. Nella nostra esperienza giuridica, volendosi escludere la nascita di un'*authority ad hoc* – che sarebbe davvero superflua in un panorama già presidiato da molteplici autorità che efficacemente potrebbero indirizzare la propria azione in tale settore – mi pare che la scelta non

[117] Art. 11, par. 1, n. 11, prop. di reg. cit.

possa che ricadere o nell'AGCM o nel Garante per la protezione dei dati personali.

La prima è più attenta alle dinamiche di mercato e alla concorrenza ed è già sensibile alle esigenze di protezione dei consumatori nelle vicende contrattuali, con controlli anche di carattere preventivo, ma non ha, per competenze e ruolo istituzionale, quella sensibilità necessaria per intervenire negli aspetti di intersezione con il diritto alla protezione dei dati personali, collocato tra i diritti fondamentali della persona e da tutelare quale diritto della personalità. Si tratta di competenza e sensibilità che invece è sicuramente riscontrabile nel Garante per la protezione dei dati personali, al quale tuttavia manca competenza e sensibilità istituzionale per le dinamiche concorrenziali.

La necessità di una convergenza tra tali istituzioni era avvertita da tempo ed ora potrebbe concretizzarsi formalmente nelle dinamiche di vigilanza sulla *data governance*. Proprio per il servizio di condivisione dei dati, personali e non personali, l'art. 12 dell'emanando regolamento richiede agli Stati membri di designare nel proprio territorio «una o più autorità competenti a svolgere i compiti relativi» alla vigilanza sulla fornitura dei servizi di condivisione dei dati, sicché la scelta migliore potrebbe essere quella di istituire una vigilanza "duale" e concorrente tra le due *authority*, come del resto si riscontra in altri settori dell'ordinamento (si pensi al settore dell'intermediazione finanziaria, con specifiche funzioni di vigilanza ripartite tra Banca d'Italia e Consob in base ad un criterio di ripartizione funzionale)[118].

La nuova proposta di regolamento sulla *data governance*, nella parte in cui disciplina il servizio di condivisione dei dati tra «titolare dei dati» e «utente dei dati», in particolare allorché la condi-

[118]Del resto un raccordo tra le diverse *authority* in materia è previsto proprio dall'art. 12, par. 2, prop. di reg. cit., ai sensi del quale «Le autorità competenti designate, le autorità per la protezione dei dati, le autorità nazionali garanti della concorrenza, le autorità responsabili della responsabili della cibersicurezza e altre autorità settoriali pertinenti si scambiano le informazioni necessarie per l'esercizio dei loro compiti in relazione ai fornitori di servizi di condivisione dei dati».

visione abbia ad oggetto dati personali per utilizzo commerciale, pone inoltre delicate questioni di sistema, nel coordinamento con la disciplina sulla *data protection* di cui al Reg. UE 679/2016, la cui applicazione viene fatta in ogni caso salva e non è pregiudicata dall'impianto normativo di cui alla richiamata proposta di regolamento[119].

4.10. *Alcune riflessioni conclusive*

Si vuole così giungere, attraverso un percorso non facile e sicuramente da modellare ulteriormente in sede applicativa, ad una «modalità nuova, "europea", di *governance* dei dati, garantendo una separazione, nell'economia dei dati, tra fornitura, intermediazione e utilizzo»[120], che non precluda ai fornitori dei servizi di condivisione dei dati la possibilità di mettere a disposizione della propria clientela un'infrastruttura tecnica specifica, dedicata all'interconnessione di "titolari dei dati" e "utenti dei dati" [121].

Preoccupa l'ambiguità del ruolo degli intermediari: visti come soggetti in grado di assicurare i diritti degli interessati nel contesto tecnologico, sembrano invece destinati, per quanto emerge dalla prassi e per le logiche in cui si inserisce il nuovo provvedimento europeo, ad esaltare la redditività dei dati personali, incoraggiandone l'utilizzo per fini commerciali che potrebbero portare ad una progressiva erosione della garanzie di tutela degli interessati.

Dovrebbero essere di monito, a tal riguardo, anche le parole critiche usate dall'*European Data Protection Supervisor* (EDPS) *nell'Opinion* n. 3/2020 *on the European strategy for data*, del 16 giugno 2020, con cui sono state esternate talune preoccupazioni concernenti le diverse modalità di intermediazione – non pienamente risolte con il testo della proposta di regolamento – sia con riguardo all'uso di *Personal Data Management Systems* o *Personal*

[119] Cfr. art. 1, par. 2, prop. di reg. cit.
[120] *Considerando* n. 25, prop. di reg. cit.
[121] *Ibidem*.

Information Managenet Systems, sia con riguardo alla figura dei *Personal Data Brokers*[122].

L'EDPS ha avuto modo di precisare, in tale contesto, che «*Personal information management systems (PIMS) are emerging as promising platforms to give data subjects more control over their personal data. Furthermore, some PIMS models could be seen as a driver for data portability as they can function as a centralized data infrastructure allowing the individuals to manage their personal data. The EDPS has already published an Opinion on Personal Information Management Systems. Therein, the EDPS stresses the need to develop technical tools and standards that make the exercise of data subjects' rights simple (e.g. with data privacy dashboards), as important means to empower the individual to manage their data. In his Opinion on PIMS the EDPS has also pointed out in particular the requirement for such systems to be fully transparent towards users and to ensure genuine user control. The EDPS notes that there are other types of data intermediaries such as data trusts and cooperatives, data marketplaces, data brokers, etc. In this regard, the EDPS emphasises the need of a clear distinction between the data intermediaries focussing exclusively on personal data and seeking to enhance individual agency, on the one hand, and those driven by economic incentives and aiming to support mainly Business to Business (B2B) data exchange, on the other hand. The EDPS considers that intermediaries aiming to empower data subjects through technical and other tools to manage the use of their data deserve consideration, further research and effective support, as they contribute to a sustainable and ethical use of data, in line with the principles of the GDPR. At the same time, the EDPS underlines the need of caution with regard to the role of data brokers that are actively engaged in the collection of huge datasets, including personal data from different sources. They tap into a variety of data sources used for data-related services, such as data that are disclosed for other unrelated purposes; data from public registers (open data), as well as data "crawled" from the Internet and social media, often in violation of data protection legislation. In this context, the EDPS*

[122] EDPS, *Opinion* No. 3/2020 *on the European strategy for data*, 16 giugno 2020, p. 6 s.

notes that the activities of big data brokers are under increased scrutiny and are investigated by a number of national data protection authorities»[123].

Con il *Data Goverance Act* l'UE intraprende una strada interessante, che cela però il rischio di svilimento dei diritti fondamentali della persona qualora la direzione intrapresa, registrata sin dai significativi mutamenti del lessico, porti ad un irreversibile processo di reificazione dei dati prima e del soggetto poi, sul quale occorre far rimanere sempre desta l'attenzione, facendo sì che in Europa rimanga viva, anche nella prassi applicativa oltre che nell'impianto di sistema, la «convinzione che l'essere umano sia e debba rimanere l'elemento centrale»[124].

[123] *Ibidem*, p. 6 s.
[124] Commissione europea, *Una strategia europea per i dati*, cit., p. 5.