GOVERNANCE OF/ THROUGH BIG DATA

Volume II

A cura di
Giorgio Resta
Vincenzo Zeno-Zencovich

Consumatori e Mercato **13**

Università degli Studi Roma Tre
Dipartimento di Giurisprudenza

Nella stessa Collana

1. V. Zeno-Zencovich (a cura di), *Cosmetici. Diritto, regolazione, bio-etica*, 2014
2. M. Colangelo, V. Zeno-Zencovich, *Introduction to European Union transport law*, I ed. 2015; II ed. 2016; III ed. 2019
3. G. Resta, V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, 2015
4. V. Zeno-Zencovich, *Sex and the contract* (II ed.), 2015
5. G. Resta, V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, 2016
6. A. Zoppini (a cura di), *Tra regolazione e giurisdizione*, 2017
7. C. Giustolisi (a cura di), *La direttiva consumer rights. Impianto sistematico della direttiva di armonizzazione massima*, 2017
8. R. Torino (a cura di), *Introduction to European Union internal market law*, 2017
9. M.C. Paglietti, M.I. Vangelisti (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2*, 2020
10. L. Scaffardi, V. Zeno-Zencovich (a cura di), *Cibo e diritto. Una prospettiva comparata*, 2020
11. A.M. Mancaleoni, E. Poillot (a cura di), *National Judges and the Case Law of the Court of Justice of the European Union*, 2020
12. E. Poillot, G. Lenzini, G. Resta, V. Zeno-Zencovich, *Data Protection in the Context of Covid-19. A Short (Hi)Story of Tracing Applications*, 2021

Università degli Studi Roma Tre
Dipartimento di Giurisprudenza

GOVERNANCE OF/ THROUGH BIG DATA

Volume II

A cura di
Giorgio Resta
Vincenzo Zeno-Zencovich

Consumatori e Mercato 13

Roma TrE-Press
2023

Coordinamento redazionale e editoriale:
Gruppo di Lavoro *Roma TrE-Press*

Collana pubblicata nel rispetto del Codice etico adottato dal Dipartimento di Giurisprudenza dell'Università degli Studi Roma Tre, in data 22 aprile 2020.

Elaborazione grafica della copertina: MOSQUITO. mosquitoroma.it

Caratteri tipografici utilizzati:
Brandon Grotesque (copertina e frontespizio)
Adobe Garamond Pro (testo)

Impaginazione e cura editoriale: Colitti-Roma colitti.it

Edizioni: *Roma TrE-Press* ©
Roma, maggio 2023
ISBN: 979-12-5977-175-9

http://romatrepress.uniroma3.it

Questo volume è pubblicato nel quadro del PRIN 2017-2017BAPSXF "Governance of/through Big Data: Challenges for European Law", finanziato dal Ministero dell'Università e della Ricerca.

L'attività della *Roma TrE-Press* è svolta nell'ambito della
Fondazione Roma Tre-Education, piazza della Repubblica 10, 00185 Roma

Presentazione della collana "Consumatori e Mercato"

Direttore: Vincenzo Zeno-Zencovich
Comitato Scientifico:
Guido Alpa, Marcello Clarich, Alberto Musso

La Collana "Consumatori e mercato", pubblicata in open access dalla Roma TrE-Press, intende essere una piattaforma editoriale multilingue, avente ad oggetto studi attinenti alla tutela dei consumatori e alla regolazione del mercato. L'intento è di stimolare un proficuo scambio scientifico attraverso una diretta partecipazione di studiosi appartenenti a diverse discipline, tradizioni e generazioni.

Il dialogo multidisciplinare e multiculturale diviene infatti una componente indefettibile nell'àmbito di una materia caratterizzata da un assetto disciplinare ormai maturo tanto nelle prassi applicative del mercato quanto nel diritto vivente. L'attenzione viene in particolare rivolta al contesto del diritto europeo, matrice delle scelte legislative e regolamentari degli ordinamenti interni, e allo svolgimento dell'analisi su piani differenti (per estrazione scientifica e punti di osservazione) che diano conto della complessità ordinamentale attuale.

****

The "Consumer and market" series published, in open access, by Roma TrE-Press, aims at being a multilingual editorial project, which shall focus on consumer protection and market regulation studies. The series' core mission is the promotion of a fruitful scientific exchange amongst scholars from diverse legal systems, traditions and generations. This multidisciplinary and multicultural exchange has in fact become fundamental for a mature legal framework, from both the market practice and the law in action standpoints. A particular focus will be given on European law, where one can find the roots of the legislation and regulation in the domestic legal systems, and on the analysis of different levels, in line with the current complexity of this legal sector.

Contents

VOLUME II

SECTION III
Big Data

SECTION IV
Data Governance

Daniel Foà
API, accesso ai conti e nuove commodities *nell'era digitale*

Giorgio Resta
Pubblico, privato, collettivo nel sistema europeo di governo dei dati

SECTION V
Data Protection and Privacy

Giorgio Resta, Vincenzo Zeno-Zencovich
Rise and Fall of Tracing Apps

SECTION III
Big Data

Vincenzo Zeno-Zencovich

Big Data e epistemologia giuridica

1. *Un nuovo "Beruf"?*

C'è un "compito per i giuristi del nostro tempo" caratterizzato dall'irrompere dei "Big Data", dell'"Internet-of-Things" e della "Data Driven Innovation", termini che vengono utilizzati come formule magiche che catturano l'attenzione di scienziati, economisti, sociologi e, ovviamente, anche dei giuristi?

Chiaramente – come dimostrato da migliaia di pagine – il principale sforzo, finora, è stato quello di versare il nuovo vino digitale negli antichi otri del diritto, in particolare quelli del diritto privato. Vi è tuttavia una ulteriore questione che appare essere assai più impegnativa e che merita di essere segnalata, lasciando alla lenta meditazione della dottrina una analisi ed un inquadramento più approfondito.

La questione è se questo scenario tecnologico relativamente recente, che sta crescendo ad un ritmo impressionante e che, apparentemente, non può essere fermato, cambia i tradizionali modelli epistemologici del giurista, ovvero il modo in cui comprende il mondo ed offre strumenti giuridici per il suo miglior funzionamento.

2. *Il precedente della statistica pubblica*

I dati sono sempre esistiti e soggetti pubblici e privati li hanno raccolti o utilizzati per millenni. Risale al 1807 la costituzione – sul modello napoleonico – dell'Ufficio statistico del Regno Italico, affidato alle cure del grande economista Melchiorre Gioja. Il fenomeno ovviamente aumenta con lo sviluppo delle società moderne e con l'uso delle tecnologie che registrano dati. In che cosa sta il cambiamento significativo? Il principale

* Questo articolo è stato originariamente pubblicato in *Dati e algoritmi. Diritto e diritti nella società digitale*, a cura di S. Faro, T.E. Frosini, G. Peruginelli, 2020, pp. 13-24.

aspetto è che la mera dimensione dei dati raccolti e memorizzati, misurabili solo in miliardi e miliardi in continua crescita, richiede nuovi strumenti per comprenderli, estrarne conoscenze, utilizzarli. Questi strumenti vanno oltre la tradizionale epistemologia – ovverosia la conoscenza di ciò che è – ma tendono ad indicare predittivamente ciò che potrebbe essere. Il diritto ha avuto per secoli una natura deontica. Ora si vorrebbe che diventasse uno strumento per realizzare soluzioni che sono state individuate attraverso analisi dei dati e che sono racchiuse in algoritmi.

Il secondo mutamento di grande rilievo è quel che può essere definito il "fattore T". In passato, decisioni di politica, e dunque normative, venivano effettuate sulla base di dati relativi al passato, su statistiche. Il termine statistica racchiude nel suo etimo il concetto di staticità. Attualmente, invece, soprattutto con lo sviluppo delle tecnologie del genere "Internet-delle-cose", i dati sono raccolti, elaborati ed analizzati in tempo reale. Ciò implica che le decisioni, anche quelle di contenuto giuridico, siano prese in tempo reale (tipicamente, chiudere una strada a causa di un incidente o di un eccessivo flusso di veicoli; il blocco all'importazione di un prodotto per ragioni sanitarie). Per poter essere tempestivi, e quindi efficaci, i procedimenti giuridici, in genere di natura amministrativa, dovranno essere pre-ordinati utilizzando i programmi predittivi che operano automaticamente sulla base di una logica semplificata. Le cautele procedurali che si riterrà di adottare verranno poste in essere in un momento anteriore, quello della elaborazione del programma. Una volta che questo sarà stato reso operativo le conseguenze giuridiche ne conseguiranno automaticamente.

Come sovente avviene con riguardo a tematiche scientifiche e tecnologiche, il livello di comprensione dei giuristi, in particolare di quelli posti nelle istituzioni dove vengono adottate le decisioni (Parlamento, amministrazioni, corti), è piuttosto limitato. In parte ciò è dovuto alla circostanza che i problemi sono complessi e non facilmente risolubili; in parte perché vi è naturale tendenza del giurista a prestare deferenza verso decisioni tecniche.

Questo atteggiamento è ancora condivisibile? Se i dati sono alla base di decisioni automatizzate di rilievo giuridico, in primo luogo in ambito pubblico[1] ma anche in quello privato[2], appare necessario comprenderne la natura, le logiche sottese alla analisi, le presunzioni e i pre-giudizi non

[1] V. Alain Supiot, *La gouvernance par les nombres. Cours au Collège de France 2012–2014*, Paris, Librairie Fayard, 2015

[2] H. Krause Hansen e T. Porter, *What Do Big Data Do in Global Governance?*, in *Global Governance*, 2017, n. 23, p. 31 ss.

dichiarati[3]. Occorre, a tal proposito, sottolineare come l'analisi dei dati sia intrinsecamente valoriale.

I dati, di per sé e soprattutto se si parla di milioni e milioni di essi, non parlano da soli, ma in genere forniscono una certa, e variabile, risposta a seconda della domanda che si pone. Ipoteticamente gli stessi dati potrebbero essere utilizzati per misurare la propensione al consumo, per finalità epidemiologiche oppure per organizzare un servizio di trasporto locale.

Per comprendere se l'uso dei dati – e degli strumenti di loro analisi – è corretto è necessario indagare e verificare la qualità dei dati, ovverosia la loro natura, le metodologie attraverso essi sono stati raccolti, gli algoritmi utilizzati per elaborarli. In tutti questi campi – che si trovano in uno stato ancora sperimentale – manca una posizione condivisa sulle metodologie appropriate e ancor meno esistono consolidati codici di condotta che si impongano o che vengano imposti a chi opera in questi campi[4]. Ciò suggerisce una qualche forma di regolazione, cogente o auto-imposta[5]6. Di certo l'atteggiamento deferenziale è di scarso uso.

Infine, proseguendo il ragionamento, è opportuno esaminare, valutare e decidere se le conclusioni analitiche tratte da alcuni dati possono essere estese ad altri settori e ad altre tipologie di decisioni. Guardando a regolamentazioni piuttosto comuni (permessi edilizi; cautele ambientali, attività commerciali) il giurista è ben consapevole delle differenze fra di esse e del fatto che le regole di un settore sono inapplicabili in un altro. Ma questa consapevolezza va estesa al mondo dei dati e al loro uso regolatorio[6].

---

[3] G. D. Bass, *Big Data and Government Accountability: An Agenda for the Future*, in *Journal of Law and Policy for the Information Society*, 2015, n. 11, p. 13 ss.

[4] Si v. il documento votato il 12.1.2017 dalla American Association for Computing Machinery, Statement on Algorithmic Transparency and Accountability (disponibile alla pagina https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_al gorithms.pdf).

[5] Vedi A. Rosenblat, T. Kneese, D. Boyd, *Algorithmic Accountability*, accessibile alla pagina https://datasociety.net/pubs/2014-0317/AlgorithmicAccountabilityPrimer.pdf; J. A. Kroll, J. Huey, S. Barocas, E. W. Felten, J. R. Reidenberg, D. G. Robinson, H. Yu, *Accountable Algorithms*, in *University of Pennsylvania Law Review*, 2017, n. 165, p. 633 ss.

[6] Vedi A. J. Casey, A. Niblett, *The Death of Rules and Standards*, in *Indiana Law Journal*, 2017, n. 92, 1401: «Advances in technology (such as big data and artificial intelligence) will give rise to this new form – the micro-directive – which will provide the benefits of both rules and standards without the costs of either. Lawmakers will be able to use predictive and communication technologies to enact complex legislative goals that are translated by machines into a vast catalog of simple commands for all possible scenarios»; nonchè J. Mitts, *Predictive Regulation*, 2014, https://ssrn.com/abstract=2411816).

3. *"Size matters"*

Si è già evidenziato come la dimensione dei dati non sia una questione meramente tecnica che possa essere risolta esclusivamente attraverso risorse digitali. Sicuramente v'è bisogno di risorse computazionali più avanzate per raccogliere e conservare la quantità sempre crescente di dati. Ma la soluzione appare più complessa[7].

Fino ad oggi la modalità più comune attraverso la quale venivano creati dei dati era attraverso la datificazione di oggetti del mondo reale: la scansione di un libro, la fotografia digitale di un oggetto, la registrazione di un evento (una conversazione, una musica, un fenomeno naturale).

In maniera molto sommaria si può immaginare che attraverso questo procedimento l'intero mondo materiale è, o può essere, datificato, creando un mondo digitale parallelo.

Un buon esempio di questa duplicazione è il servizio di Google Street View che offre una riproduzione di una città da molteplici prospettive. Anche se in generale il servizio funge da mappa, la quantità di informazioni contenute nei dati (gli alberi sulla strada, i posteggi, i colori dei palazzi, la presenza di esercizi commerciali, ecc.) va ben oltre la mera indicazione stradale e letteralmente trasporta l'utente in un determinato luogo. La digitalizzazione degli oggetti, ancorchè sia ben lungi dall'essere completata, comporta una duplicazione del mondo reale, un duplicato che può essere utilizzato da qualsiasi luogo e in qualsiasi momento, da un numero illimitato di persone, le quali possono adattare i dati ai propri bisogni ed interessi e trasformarli in qualcosa di nuovo e differente[8].

A guardare le cose dall'esterno si direbbe che gli oggetti del mondo reale, una volta datificati, hanno quel che si potrebbe definire "una seconda vita", e i due spazi (fisico e digitale) costantemente fanno riferimento l'uno all'altro. A ciò si aggiunga che ancorchè versioni digitali di oggetti, come un libro, un quadro, una esecuzione musicale, sono esistite da decenni, metterle in un contesto interattivo nel quale si mescolano con milioni di altri dati serve ad evidenziare la complessità ma anche le significative differenze. Si potrebbe definire questa nuova entità la "datasfera" la quale è

[7] Ho cercato di sviluppare più ampiamente questi concetti in J-S Bergé, S. Grumbach, V. Zeno-Zencovich, *The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance*, in *European Journal of Comparative Law and Governance*, 2018, n. 5, p. 144 ss.

[8] Può essere utile confrontare la messe di dati e di considerazioni contenuti nel rapporto dell'OCSE, *Data-driven Innovation for Growth and Well-being* (October 2014), con la situazione attuale per verificare quanto la situazione sia cambiata in cinque anni.

la replica digitale del mondo e di ciò che si conosce dell'universo.

La datasfera ha le proprie regole. Non si vuole sostenere la tesi libertaria formulata agli albori della rete Internet che la definiva uno spazio letteralmente utopico sottratto alle interferenze del diritto nazionale o soprannazionale. Ormai si è compreso che il c.d. ciberspazio è un ambiente intensamente regolato nelle sue infrastrutture, nei suoi modi di comunicazione, nei suoi contenuti.

Quel che si vuole mettere in luce è che la datasfera, che potrebbe metaforicamente descriversi come un oceano nel quale le reti di comunicazioni costantemente riversano, ogni istante, milioni di dati in un flusso ininterrotto, è scarsamente governabile. Rispetto alla metafora però la differenza è che gli oceani sono dimensionalmente relativamente stabili, mentre la datasfera cresce con una progressione accelerata. Non solo gli apparati che producono dati stanno aumentando nell'ordine di milioni in poco tempo (dai contatori di energia agli autoveicoli, dai sensori utilizzati in agricoltura, alle applicazioni domotiche), ma i dati, una volta immessi nella datasfera, si mescolano con altri dati, producendo nuovi dati in un procedimento senza fine.

Si potrebbe dire che mentre gli esseri umani stanno cercando di scoprire l'universo sfidando l'infinito, essi stanno creando, su questo pianeta, un mondo digitale infinito costituito dai dati.

Quali sono le implicazioni per il diritto?

La prima, ovvia, considerazione è che governare attraverso regole il mondo digitale non è la stessa cosa che governare il mondo fisico.

Stabilire regole per condotte umane è diverso da stabilire regole (ma quali?) che dovrebbero controllare procedimenti quasi interamente automatici in un contesto digitale.

La seconda osservazione è riferita alla ubiquità o alla indeterminata collocazione fisica dei dati. È estremamente difficile stabilire dove i dati sono conservati, e se sono conservati in un unico "spazio digitale" (ammesso che del termine si possa fornire una definizione condivisa). La questione ha delle ovvie implicazioni con riguardo al diritto applicabile, diritto che non è – o non è in prevalenza – diritto privato, ma più spesso diritto pubblico nelle sue molteplici sfaccettature amministrative e regolatorie. Di fatti, mentre vi è un ampio apparato normativo e di decisioni giurisprudenziali le quali trattano i problemi di conflitti di legge e di giurisdizione in materie privatistiche, mancano analoghe soluzioni nel campo del diritto amministrativo il quale è inevitabilmente legato ai confini della giurisdizione nazionale e non è in grado di esplicare

effetti al di fuori di questa[9]. Per il mare, il cielo, lo spazio extraterrestre vi sono puntuali convenzioni internazionali. Per la datasfera stiamo ancora cercando di definirla.

Infine, occorre considerare che la datasfera appare essere governata – a differenza del mare, dei cieli e dello spazio – interamente da strumenti tecnologici (hardware, software, reti di comunicazione, ecc.) creati da umani. Si potrebbe forse inferirne che una volta si sia stabilito che cosa gli esseri umani e le loro entità giuridiche possono (o non possono) fare nella datasfera si potrebbe costruire un sistema ordinato di regole. Va tuttavia osservato che non solo queste regole sono prevalentemente di natura tecnica, ma soprattutto che l'intero sistema è in maniera crescente fondato su procedimenti di auto-apprendimento. Benché siano ancora lontani dal replicare la complessità della mente umana, tuttavia l'intelligenza artificiale, e quindi la possibilità per delle macchine di replicare processi mentali attraverso la autonoma acquisizione di dati, è assai difficile da fermare o regolare.

I giuristi non temono nuovi mondi – geografici o artificiali – e dispongono degli strumenti per affrontarli e mettere ordine in ciò che appare essere solo caos. Tuttavia ciò richiede un uso appropriato delle tassonomie, evitando le trappole dell'iniziatico dialetto digitale o dello *slang* giovanilistico, espressi in termini vaghi ed indeterminati, ovviamente inglesi.

La prima sfida consiste dunque nell'individuare le situazioni tenendo conto dei rapidi mutamenti tecnologici.

Mentre è chiaro che prima avvengono i fatti, poi arriva il diritto, non si può fare a meno di ricordare ai non giuristi che la logica e il linguaggio formale non sono una esclusiva delle scienze informatiche, ma anche pilastri fondamentali dell'edificio del diritto. Come nell'informatica si rigettano nozioni volatili che non conducono da nessuna parte, così anche nel diritto occorre definire, distinguere, mettere ordine.

Il diritto potrebbe essere definito un proto-software e questa è la ragione per la quale l'informatica giuridica si è sviluppata così rapidamente come specifica branca del sapere e di ricerca.

Dall'altra parte occorre anche evitare di usare le esistenti e tradizionali istituzioni giuridiche (proprietà, contratto, procedure amministrative) come un letto di Procuste sul quale forzatamente sdraiare gli elementi del nostro mondo tecnologico.

Vi sono altre istanze che appaiono essere più impellenti.

[9] J. de Jong-Chen, *Data Sovereignty, Cybersecurity, and Challenges for Globalization*, in *Georgetown Journal of International Affairs*, 2015, n. 16, p. 112 ss.

Il diritto è un prodotto sociale e non può esistere se non è seguito, volontariamente o grazie ad effettivi strumenti di conformazione, da una comunità. Le tecnologie digitali non solo consentono di conoscere ed applicare il diritto, dovunque e in qualsiasi momento, ma spesso suggeriscono, se non addirittura impongono, una regola da seguire: l'esempio più banale è quello dei "campi" digitali che è obbligatorio riempire se si vuole un certo risultato (la prenotazione, l'acquisto, ecc.). Ma questo obbligo non è certo imposto dalla legge, ma dal soggetto che ha realizzato il modulo informatico e non consente deviazioni o variazioni.

È possibile dunque preconizzare un crescente processo di applicazione automatizzata delle regole giuridiche, già particolarmente esteso nel settore tributario ed in quello della sicurezza sociale, sia nelle relazioni degli individui con le autorità e tra individui.

La combinazione fra regole giuridiche e dati porta nel nostro campo visuale le c.d. norme granulari e, per usare una espressione che in realtà rivela un ossimoro, gli "smart contracts".

Le norme perdono la loro caratteristica di generalità e sono ritagliate su misura sulla identità del soggetto, identità nota attraverso la quantità di dati personali di cui il soggetto che crea la regola (privato, ma anche pubblico) dispone.

Si può e si deve indagare sul ruolo che le analisi predittive hanno nella applicazione delle norme. L'esempio più evidente in cui esse sono già ampiamente utilizzate è quello delle indagini di polizia che mirano a restringere un gruppo di persone sospette o individuare legami fra persone sospette e persone insospettabili.

Su un piano più comune, peraltro, analisi predittive sono utilizzate – e lo saranno sempre di più – nella selezione del personale, nei test di ammissione alla scuola e all'università e in altri contesti quali diritti individuali e rapporti trasparenti con le pubbliche autorità sono in gioco. Qui non vi è direttamente la applicazione di una norma, ma piuttosto la determinazione dello *status* della persona, che corrisponde ai dei "tipi" algoritmicamente pre-determinati. La capacità dipende dunque da modelli sociali disegnati altrove – in particolare in un paese diverso, con diverse dinamiche e strutture – e trasposti automaticamente in un contesto che può essere molto differente.

4. *Una logica inferenziale*

Si è già messa in luce la circostanza che i "Big Data" ed il contesto che determinano hanno già modificato lo stato del diritto ed il modo attraverso il quale esso è posto in operazione. Meritano di essere segnalati tre ulteriori aspetti[10]:

a) Per millenni il ragionamento è stato fondato su quel che si può chiamare una logica causale bene espressa dal binomio se/quindi[11]. I "Big Data" per via delle loro dimensioni, della loro varietà, della velocità alla quale sono raccolti ed elaborati sono, solitamente, analizzati secondo una logica inferenziale, espressa dal binomio se/allora forse. Essa, naturalmente, apre la strada a molteplici soluzioni, ma solitamente verrà considerata solo quella che, sulla base dei dati disponibili, è considerata la più probabile. Anche in passato regole giuridiche sono state applicate sulla base di ragiona ragionamenti *lato sensu* probabilistici: le "massime di esperienza", l'*id quod plerumque accidit*, le finzioni, le presunzioni. Ma esse erano, di solito, filtrate e ponderate da un soggetto umano che doveva decidere uno ed un solo caso. Quel che cambia ora è la generalizzazione che passa dal caso singolo a tutti quei casi accomunati *a priori* da taluni elementi ricorrenti.

Da regola per il caso concreto a norma generale. Mentre questa prevedibilità non presenta eccessivi problemi nel mondo degli scambi digitali (il miglior esempio è quello dei portali di vendita on-line: «I clienti che hanno acquistato A hanno considerato se comprare anche B»), quando viene applicato alle norme giuridiche esso mette in dubbio principi

[10] Cfr. R. Kitchin, *Big Data, new epistemologies and paradigm shifts*, in *Big Data & Society*, April-June 2014, p. 1 ss., disponibile alla pagina http://eprints.maynoothuniversity.ie/5364/1/RK_big%20data.pdf; M. Frické, *Big Data and its Epistemology*, in *Journal of the Association for Information Science and Technology*, 2015, n. 66, p. 651 ss., disponibile alla pagina https://ischool.arizona.edu/sites/si.arizona.edu/files/FrickeBigDataPaperShorterFormat.pdf.

[11] Si v. il *Menone* di Platone: «Possedere una delle statue di Dedalo che sia slegata non è di grande valore, è come possedere uno schiavo che fugge - infatti non se ne sta fermo -; se invece è legata vale molto: perché queste opere sono molto belle. A proposito di cosa sto dicendo questo? A proposito delle opinioni vere. Infatti, anche le opinioni vere per tutto il tempo in cui restano salde sono un bel tesoro e realizzano ogni bene. Ma esse non vogliono rimanere salde per molto tempo, ma fuggono dall'anima dell'uomo, per cui non hanno grande valore, fin tanto che non siano legate con un ragionamento sulla causa. Questo, Menone, amico mio, è reminiscenza, come abbiamo ammesso prima nei nostri discorsi. Quando siano legate, diventano dapprima scienza e poi stabili: ed è per questo che la scienza è più apprezzata di una giusta opinione, e la differenza tra scienza e giusta opinione sta nella connessione».

profondamente radicati. Ogni regola è composta di vari elementi più o meno rigidamente definiti (molto rigorosamente nel diritto penale, meno negli altri casi). Se uno o più di tali elementi manca, la norma non si potrà applicare. Tenendo conto delle inevitabili differenze che la casistica offre vi è una costante interazione fra regola generale/eccezioni generali/regola speciale.

b) Il ragionamento inferenziale spazza via tutto ciò, e prospetta un diverso modo di pensare ed agire. Diventerà comune anche nel ragionamento giuridico, generalizzando decisioni che sono state pensate su casi paradigmatici, senza tenere in considerazione i casi anomali? Miliardi di dati sono difficili da analizzare ed è difficile esprimere il risultato delle ricerche che su di essi sono stati effettuati. Ciò ha portato al crescente sviluppo ed uso di analisi visuali ("visual analitics" o "data visualization"), altrimenti dette "infografiche".

Queste immagini colorate attraggono l'attenzione e dovrebbero trasmettere il significato dei dati. Qui sorgono immediatamente numerosi dubbi. In primo luogo, viene da chiedersi se tali presentazioni effettivamente forniscono la rappresentazione veritiera dei risultati della ricerca effettuata sui dati oppure se, per esigenze estetiche e di apparente chiarezza, l'intera immagine è stata fortemente semplificata (ad es. con contorni netti, evitando sfumature di colori, omettendo le risultanze percentualmente marginali, fornendo una dimensione o una prospettiva parziale). In secondo luogo, non possiamo dimenticare che comunicare attraverso immagini è diverso – molto diverso – dal cercare di spiegare un concetto o una situazione con le parole che si rivolgono all'intelletto[12]. Se si applica la dicotomia intellettuale/visuale al ragionamento e alle regole giuridiche,

[12] V. Aristotele, *Sull'anima*, che nelle parti 3, 7 e 9 analizza in dettaglio il rapporto che esiste fra pensiero, comprensione, conoscenza, immagini e immaginazione, al punto che «l'anima non pensa mai senza avere una immagine». E *Sull'interpretazion*e (cap. I) si esprime in questi termini «Dunque, i suoni della voce sono simboli delle affezioni che hanno luogo nell'anima, e le lettere scritte sono simboli dei suoni della voce. Allo stesso modo poi che le lettere non sono le medesime per tutti, così neppure i suoni sono i medesimi; tuttavia, suoni e lettere risultano segni, anzitutto, delle affezioni dell'anima, che sono le medesime per tutti e costituiscono le immagini di oggetti, già identici per tutti». Allo stagirita si può aggiungere David Hume, nella sua *Enquiry Concerning Human Understanding* (1748): «Perceptible objects always have a greater influence on the imagination that anything else does, and they readily convey this influence to the ideas to which they are related and which they resemble» (Section. 5); e «Philosophy teaches us that images (or perceptions) are the only things that can ever be present to the mind, and that the senses serve only to bring these images before the mind and cannot put our minds into any immediate relation with external objects» (Section 12).

si può dubitare che il diritto e le sue molteplici complessità e sfumature possano essere espresse attraverso delle immagini. E che le innumerevoli variazioni nella casistica giurisprudenziale – la quale è la prima fonte di "Big Data" giuridici – possano essere correttamente e fedelmente rappresentate attraverso strumenti di "data visualization"[13].

d) L'ultima considerazione che si vuole svolgere con riguardo alla rivoluzione dei "Big Data" è l'emergenza di una nuova classe di decisori politici. Fino alla metà del XX secolo le decisioni di *policy* (con ciò intendendo di politica del diritto, ponendo l'accento sul primo sostantivo) erano prese, prevalentemente, da soggetti i quali avevano una formazione giuridica e sapevano "fare cose con regole".

Dopo la Seconda guerra mondiale gli economisti sono entrati in scena influenzando profondamente grandi e piccole decisioni di governo e di amministrazione. Ora questo ruolo viene, in maniera crescente, occupato da informatici il cui status professionale è incerto, il cui ruolo non è trasparente, e la cui attività non appare essere assoggettata a principi professionali e deontologici. In altre parole, una norma è conosciuta e conoscibile dai cittadini – di qui la fondamentale esigenza della pubblicità delle leggi e degli atti normativi – e chiunque può contestarla – in particolare in un giudizio – sulla base di altre norme, spesso di rango gerarchico sopra-elevato. Ma ciò è particolarmente difficile se dietro la norma vi sono dati ed algoritmi. La "data accountability" – la responsabilità per la qualità dei dati che utilizzano e per la correttezza delle procedure che sono utilizzate – diventa dunque una questione centrale in una moderna e tecnologica democrazia. Ma questa responsabilità è non solo di natura tecnica ma anche, e in primo luogo, deontica[14]. Quali pre-giudizi o pre-comprensioni guidano le inferenze che si traggono dall'analisi dei dati: l'età, il sesso, l'etnia, il domicilio? Quali sono gli assunti su cui si fonda una analisi predittiva? Vi sono, e quali sono, obiettivi politico-sociali perseguiti: efficienza? Equità? Uguaglianza? Giustizia sociale?

[13] Sia consentito rinviare a V. Zeno-Zencovich, *Through a lawyer's eyes. Data visualization and legal epistemology*, in E. Degrave, C. de Terwangne, S. Dusollier, R. Queck (a cura di), *Law, norms and freedoms in cyberspace - Liber amicorum Yves Poullet*, Bruxelles, Larcier, 2018, p. 459 ss.

[14] Per una posizione estrema v. C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York, Crown, 2016.

Vincenzo Zeno-Zencovich

Liability for data loss

1. *Datasphere*

Our societies are, already, growingly and irreversibly, data societies. Each year zettabytes (i.e., 1000^7 = 1.000.000.000.000.000.000.000) of data are generated. Once upon a time humans interacting with digital devices were the main sources of data. With the development of Internet-of-Things (IoT) billions and billions of objects, animals, plants, buildings are already and will be generating, communicating, storing further data, every instant of every day.

All this data will be collected, aggregated, processed. Mainframe computers will generate further data that will be combined with other data, in a never-ending process.

This 'datasphere'[1] is not only potentially infinite, but is the digital representation of everything we can datify, not only on this planet but in the whole universe (e.g., the data which is sent to us by spacecrafts further and further away from the Earth).

An individual, a building, a forest exist in their physical elements. But they exist also as the whole of the data which represent them, and what is even more important, in time, in space and in their relations.

In this context, what do we mean with 'data loss'? A 19th century dogmatic lawyer would have probably written a whole book on the topic, thoroughly investigating up-stream to the sources of data, and down-stream to their unlimited uses to understand where the lost data have ended up and, if any, redress is available.

The purpose of this chapter is, decidedly, less ambitious, and much more down-to-earth.

---

[*] This article was first published in the *Research handbook in data science and law*, pp. 39-54.

[1] J-S Bergé, S. Grumbach, V. Zeno-Zencovich, *The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance*, in *EJCL&G*, 5, 144, 2018. Previously, J-S Bergé, S. Grumbach, *The Datasphere and the Law: New Space, New Territories*, 2016, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2868904> (accessed on Mar. 19, 2018).

2. *'Loss'*

The first point one should make is what we mean for 'data loss'? When does this phenomenon become of some significance? To borrow an example from the physical world, we all lose hair – which incidentally contains very revealing data on our DNA – but thank goodness nobody, not even the staunchest supporter of pervasive regulation, has considered it worthy of legal intervention.

And prior to the issue of relevance a civilian asks himself/herself what are the ownership issues. One can 'lose' only what one owns. One cannot 'lose' the dust on one's shoes, the insect flying in our room, the shade of our body[2].

'Ownership' of data, however, is far from a settled issue[3].

In the first place, does one 'own' one's own data? 'Own', in the sense that one has a property right (in a civilian sense) over such data?[4] Or does one have the right to control certain (not all) uses of such data and to prevent them in certain cases? Again a civilian might qualify this as a limited *ius arcendi*, but not as a fully-fledged property right. Probably it might be more appropriate to use a less engaging term: entitlement[5].

Setting aside personal data – in itself a fuzzy notion – does one 'own' the

[2] The literary reference is to A. von Chamisso's short story on Peter Schlemihl who sold his shadow to the devil.

[3] 'Ownership' of data is thoroughly investigated (and challenged) by F. Mezzanotte, *Access to Data: The Role of Consent and the Licensing Scheme*, in S. Lohsse, R. Schulze, D. Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools, Hart/Nomos*, 2017, p. 159. Similar critical views are expressed by S. van Erp, *Ownership of Digital Assets and the Numerus Clausus of Legal Objects*, Maastricht European Private Law Institute Working Paper No. 2017/6 (October 1, 2017), available at SSRN: <https://ssrn.com/abstract=3046402> (accessed on Mar. 19, 2018). I have tried to set out a number of related issues in V. Zeno-Zencovich, G. Giannone Codiglione, *Ten Legal Perspectives on the Big Data Revolution*, in *Concorrenza e Mercato*, vol. 23, 29, 2016. See also D. L. Burk, *Privacy and Property in the Global Datasphere*, (April 28, 2005), available at SSRN at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=716862> (accessed on Mar. 19, 2018). The 'property right' over data approach is instead amply presented in N. Purtova, *Property Rights in Personal Data: A European Perspective*, Oisterwijk, BOXPress, 2011 (in particular in chapter 10, pp. 236 ff.)

[4] For those brought up in a Roman law context it would come natural to quote Ulpian: *Dominus membrorum suorum nemo videtur*.

[5] In the same terms see S. van Erp, cited in note 3: 'This does not mean that no primary right (in the sense of the maximum of powers, rights, privileges and immunities) exists, but it is not ownership, but entitlement.'

data one holds?[6] Does one 'own' data which – so to speak – are in the public domain: what time it is, the weather, statistical data, etc? When such data is organized might it be protected, in the European Union, by a *sui generis* right?[7] But if it is not structured? When does one become the 'owner' of data? When one generates them (e.g., data on the sales of a firm)? When they are stored in a portion of digital memory to which one has exclusive access?

Entitlement to data becomes a relevant issue – as we shall see – when discussing remedies (mostly damages) for the loss of data.

Further issues arise from the intangible nature of data, which economists generally qualify as 'public goods' in the sense that they are not rivalrous and non-consumable. This means not only that many other persons or entities may share the same data, but also that, quite commonly, data are generated by two or more persons who can claim an equal entitlement:[8] in a family relation the status of spouse, parent, son, brother, etc. necessarily implies the existence of data pertaining to someone else[9]. The parties of a contract (buyer/seller; landlord/tenant; employer/employee) necessarily must share the data concerning their relationship[10].

We therefore have data which is intrinsically common to two or more entities. If a bank loses all the data concerning its accounts, it loses also the data related to its clients.

These caveats must be taken into account when analysing the legal implications of data losses.

---

[6] For a radical – but not altogether removed from reality – view see Joshua A. T. Fairfield, *Owned. Property, Privacy, and the New Digital Serfdom*, Cambridge U.P. 2017.

[7] Arts 7–11 of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases

[8] The issue was pioneeringly set out by the present European Data Protection Supervisor, Giovanni Buttarelli in his *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, Giuffrè, 1997, p. 194: 'Does the law necessarily imply that the use of data be exclusively and necessarily individual, or can one imagine that forms of shared entitlement are allowed between two physical persons who are in a very tight relationship of interests.' For further developments see V. Zeno-Zencovich, *La 'comunione' di dati personali. Un contributo al sistema dei diritti della personalità*, in *Il diritto dell'informazione e dell'informatica*, 6, 2009.

[9] Not to speak about genetic data which can 'belong' to several generations: see the Iceland Supreme Court, 7.11.2003, n. 151, *Gudmunsdottir v Iceland* (available at <https://epic.org/privacy/genetic/iceland_decision.pdf>).

[10] 'Shared data' is a term commonly used in database science and practice: see S.E. Coull, E. E. Kenneally, *Toward a Comprehensive Disclosure Control Framework for Shared Data*, in *IEEE International Conference on Technologies for Homeland Security* (November 2013, Boston, MA) available at SSRN: <https://ssrn.com/abstract=2326264> (accessed on Mar. 19, 2018). In the cases that are presented here, however, data is 'shared' because it is 'common'.

3. *Contractual Remedies*

In a considerable amount of cases data are stored in/on digital facilities of third parties with which the entitled person or entity has a contractual relationship.

One is not so much interested in those complex contracts – usually business-to-business – which are the natural development of the outsourcing contracts which were introduced over 30 years ago to enable many businesses to avoid costly investments in computers and related specialized personnel by paying a periodical fee to a digital service provider who not only stored the data but also processed it (typically for pay-rolls, balance sheets, tax forms etc.)[11]. The fact that the computing capacity is multiplied; that the service is rendered often through 'cloud' techniques[12]; and that data is collected and forwarded through a multitude of devices, does not seem to change the legal substance of the problem.

Is the service provider liable for the loss of data? This depends on the size of the parties, if they bargain at arm's length, or if there is significant unbalance in favour of the service provider. In the latter case one can expect widespread use of exemption or limitation clauses similar to these already existing in most outsourcing contracts[13]. As most of these providers are global operators standard terms will be the same mostly in every country, and no effort will be made to adapt them to the specific jurisdiction.

One can assume that in most cases the entity entitled adopts technical measures (e.g., back-up) to minimize data losses, or buys insurance. And the same can be said of the service provider[14]. More specifically one can

[11] See G. Kimball, *Outsourcing Agreements: A Practical Guide*, OUP 2010.

[12] See S. Bradshaw, C. Millard, I. Walden, *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, in Queen Mary School of Law Legal Studies Research Paper No. 63/2010 (Sept. 2010), available at SSRN: <https://ssrn.com/abstract=1662374>: 'Our survey found however that most providers not only avoided giving undertakings in respect of data integrity but actually disclaimed liability for it.' (at p. 21). Similar conclusions in R. H. Weber, D. N. Staiger, *Cloud Computing: A cluster of complex liability issues*, 20(1), 2014, Web JCLI. One must add that the contractual terms for the 'cloud' are shrouded in the mist, in the sense that they are not available when one accesses the main websites. This fact, in itself, is revealing.

[13] One cannot take it for granted that such limitation clauses will be struck down in B2B contracts: see e.g., the decision by The Hague Gerechtshof (28.9.2016), available at <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHDHA:2016:2690> (accessed on Mar. 19, 2018), which has held a similar clause valid and rejected the claim for damages of the client of the service provider.

[14] See the recent Dutch decision of the Limburg Rechtbank of 5.7.2017, which clari-

reasonably expect that state-of-the-art diligence implies the implementation by the professional service provider of high-level safety (to avoid losses) and security (to avoid breaches) procedures. One should, however, consider that in some cases contributory negligence of the person or entity which is availing itself of the service could be invoked. Clearly this depends on factual situations: if some part of the computer infrastructure is within the control of the data generator, one might require that the latter enact safety measures, including back-ups. But if it is using mainframe and software services of the provider (and therefore disposes only of end-user terminals) it is even difficult to imagine how this could be possible.

What deserve more attention are less formalized relations between small businesses and service providers and between common individuals and service providers.

In the first place it would appear that users of on-line services have a contractual relation with the service provider[15]. It is quite immaterial that the small business or the individual does not sign any contract or pays some monetary consideration. Apart from those who believe in the fairy tale that these services 'are free and will always be', users generally remunerate the services they receive through the flow of data they provide[16] (the typical check-test is the growing amount of web-based services which are not

fies the back-up obligations of a service provider. The decision is available at <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBLIM:2017:6454> (accessed on Mar. 19, 2018).

[15] This statement however requires a number of clarifications which are clearly set out by R. Janal, *Fishing for an Agreement: Data Access and the Notion of Contract*, in S. Lohsse, R. Schulze, D. Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools*, Hart/Nomos, 2017, p. 271.

[16] This approach has (finally) been accepted by the EU institutions: see the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content: Art. 3 (Scope): This Directive shall apply to any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money
[i]n the form of personal data or any other data. It is however challenged in the Opinion of the EDPS of March 14, 2017 (at § 14): 'Personal data cannot be compared to a price, or money. Personal information is related to a fundamental right and cannot be considered as a commodity'. 'One cannot monetise and subject a fundamental right to a simple commercial transaction, even if it is the individual concerned by the data who is a party to the transaction' (§17). For a first presentation of personal data as valid consideration for the provision of services see V. Zeno-Zencovich, *I diritti della personalità dopo la legge sulla protezione dei dati personali*, in *Studium Iuris* 466, 1997, p. 469. In order to obtain the consent of the interested person [to the processing of personal data] businesses are generally willing to provide some kind of remuneration, albeit modest, which is a sure index of the economic nature of the conferral of data, and therefore of its qualification as a contract.

provided if the user does not accept cookies)[17].

Even if the entitled person or entity owns a device (computer, tablet, hand-set) on which the data, apparently, is stored and is available, it is quite common that such data is not – or is not entirely – in the direct and immediate command-and-control of such person or entity[18], but in most cases is memorized in an external digital memory accessible on-line. Again the check-test is the availability of such data when there is no internet network connection.

In these cases the relationship between user and service provider are, apparently, regulated by neatly tucked away 'general terms of service' which one finds in fine print at the bottom of the home-page of the provider and which, quite normally, are ignored by any sane user. It is worthwhile reproducing some of the relevant provisions on data loss or, which is tantamount, on denial of service. It is sufficient to peruse the main providers of search engines or of social media to encounter a flourish of clauses which exclude any sort of liability.

This is how the rule is expressed in Facebook's terms of service: 'We do not guarantee that Facebook will always be safe, secure or error-free or that Facebook will always function without disruptions, delays or imperfections'[19].

[17] The point has been aptly made by the Italian Competition and Consumer Authority in the WhatsApp II case (11.5.2017). Available at <http://www.agcm.it/component/joomdoc/allegati-news/PS10601_scorrsanz_omi.pdf/download.html> (accessed on Mar. 19, 2018).

[18] But see the remarks of C. Lazaro, D. Le Métayer, *Control over Personal Data: True Remedy or Fairy Tale?* (April 14, 2015), available at <https://arxiv.org/ftp/arxiv/papers/1504/1504.03877.pdf> (accessed Mar. 19, 2018).

[19] Art 15.3 Facebook Statement of Rights and Responsibilities:

> We try to keep Facebook up, bug-free, and safe, but you use it at your own risk. We are providing Facebook as is without any express or implied warranties including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We do not guarantee that Facebook will always be safe, secure or error-free or that Facebook will always function without disruptions, delays or imperfections. Facebook is not responsible for the actions, content, information, or data of third parties and you release us, our directors, officers, employees, and agents from any claims and damages, known and unknown, arising out of or in any way connected with any claim you have against any such third parties. If you are a California M4619- resident, you waive California civil code §1542, which says: A general release does not extend to claims which the creditor does not know or suspect to exist in his or her favor at the time of executing the release, which if known by him or her must have materially affected his or her settlement with the debtor. We will not be liable to you for any lost profits or other consequential,

In Google's terms of service the same principle is so stated: 'We do not make any commitments about the content within the Services, the specific functions of the Services or their reliability, availability or ability to meet your needs. We provide the Services "as is".'[20]

special, indirect, or incidental damages arising out of or in connection with this statement or Facebook, even if we have been advised of the possibility of such damages.

Our aggregate liability arising out of this statement or Facebook will not exceed the greater of one hundred dollars ($100) or the amount you have paid us in the past twelve months. Applicable law may not allow the limitation or exclusion of liability or incidental or consequential damages, so the above limitation or exclusion may not apply to you. In such cases, Facebook's liability will be limited to the fullest extent permitted by applicable law.

[20] Our Warranties and Disclaimers

We provide our Services using a commercially reasonable level of skill and care and we hope that you will enjoy using them. But there are certain things that we do not promise about our Services.

Other than as expressly set out in these terms or additional terms, neither Google nor its suppliers or distributors makes any specific promises about the Services. For example, we do not make any commitments about the content within the Services, the specific functions of the Services or their reliability, availability or ability to meet your needs. We provide the Services 'as is'.

Some jurisdictions provide for certain warranties, like the implied warranty of merchantability, fitness for a particular purpose and non-infringement. To the extent permitted by law, we exclude all warranties.

Liability for our Services

When permitted by law, Google and Google's suppliers and distributors will not be responsible for lost profits, revenues or data, financial losses or indirect, special, consequential, exemplary or punitive damages.

To the extent permitted by law, the total liability of Google and its suppliers and distributors for any claims under these terms, including for any implied warranties, is limited to the amount that you paid us to use the Services (or, if we choose, to supplying you with the Services again).

In all cases, Google and its suppliers and distributors will not be liable for any loss or damage that is not reasonably foreseeable. We recognise that in some countries, you might have legal rights as a consumer.

If you are using the Services for a personal purpose, then nothing in these terms or any additional terms limits any consumers' legal rights which may not be waived by contract.

Business uses of our Services

If you are using our Services on behalf of a business, that business accepts these terms. It will hold harmless and indemnify Google and its affiliates, officers, agents and employees from any claim, action or proceedings arising from or related to the use of the Services or violation of these terms, including any liability or expense arising from claims, losses, damages, judgements, litigation costs and legal fees.

Twitter's terms of service are not dissimilar: 'The Twitter Entities make no warranty or representation and disclaim all responsibility and liability for (. . .) any harm to your computer system, loss of data, or other harm that results from your access to or use of the Services or any Content.'[21]

Flickr's terms of service are equally peremptory and relevant, considering the nature of the data (photos) liable to be lost: 'Your use of Flickr APIs is

[21] Art 5 Twitter Terms of Service

'Disclaimers and Limitations of Liability

> The Services are Available 'AS-IS'
>
> Your access to and use of the Services or any Content are at your own risk. You understand and agree that the Services are provided to you on an 'AS IS' and 'AS AVAILABLE' basis. The 'Twitter Entities' refers to Twitter, its parents, affiliates, related companies, officers, directors, employees, agents, representatives, partners, and licensors. Without limiting the foregoing, to the maximum extent permitted under applicable law, the twitter entities disclaim all warranties and conditions, whether express or implied, of merchantability, fitness for a particular purpose, or non-infringement. The Twitter Entities make no warranty or representation and disclaim all responsibility and liability for: (i) the completeness, accuracy, availability, timeliness, security or reliability of the Services or any Content; (ii) any harm to your computer system, loss of data, or other harm that results from your access to or use of the Services or any Content; (iii) the deletion of, or the failure to store or to transmit, any Content and other communications maintained by the Services; and (iv) whether the Services will meet your requirements or be available on an uninterrupted, secure, or error-free basis. No advice or information, whether oral or written, obtained from the Twitter Entities or through the Services, will create any warranty or representation not expressly made herein.

Limitation of Liability

> The Twitter Entities shall not be liable for any indirect, incidental, special, consequential or punitive damages, or any loss of profits or revenues, whether incurred directly or indirectly, or any loss of data, use, good-will, or other intangible losses, resulting from (i) your access to or use of or inability to access or use the services; (ii) any conduct or content of any third party on the services, including without limitation, any defamatory, offensive or illegal conduct of other users or third parties; (iii) any content obtained from the services; or (iv) unauthorized access, use or alteration of your transmissions or content. The limitations of this subsection shall apply to any theory of liability, whether based on warranty, contract, statute, tort (including negligence) or otherwise, and whether or not the twitter entities have been informed of the possibility of any such damage, and even if a remedy set forth herein is found to have failed of its essential purpose.
>
> Some jurisdictions do not allow exclusion of implied warranties or limitations on the duration of implied warranties, so the above disclaimers may not apply to you in their entireties, but will apply to the maximum extent permitted by applicable law.

at your own discretion and risk, and you will be solely responsible for (. . .) any damage to your computer system or loss of data.'[22]

Are these clauses valid? In an EU law perspective they are radically void when they purport to regulate a consumer/professional relationship inasmuch they are in blatant violation of the Unfair Terms Directive,[23] and specifically of its black-list clauses set out in the Annex. Practically all the letters, from a) to q), could be applied to the cited standard terms. It is sufficient here to refer to letter b): 'Inappropriately excluding or limiting the legal rights of the consumer vis-à-vis the seller or supplier or another party in the event of total or partial non-performance or inadequate performance by the seller or supplier of any of the contractual obligations.'

One can therefore assume that – with all the doubts on evidence and on liquidation of damages which shall be seen further on – the service provider is entirely liable for losses due to its professional negligence, unless it can prove typical exonerating circumstances such as force majeure, State intervention, unavoidable events (such as unprecedented and unforeseeable hacking attempts or virus infections).

If provision of data for the digital services rendered are considered an adequate consideration for establishing the existence of a contract[24] at that

[22] 7. Disclaimer of Any Warranty.

> Some of the Flickr APIs may be experimental and not tested in any manner. Flickr does not represent or warrant that any Flickr APIs are free of inaccuracies, errors, bugs, or interruptions, or are reliable, accurate, complete, or otherwise valid. the Flickr APIs are provided 'as is' with no warranty, express or implied, of any kind and Flickr expressly disclaims any and all warranties and conditions, including, but not limited to, any implied warranty of merchantability, fitness for a particular purpose, availability, security, title and/or non-infringement. Your use of Flickr APIs is at your own discretion and risk, and you will be solely responsible for any damage that results from the use of any Flickr APIs including, but not limited to, any damage to your computer system or loss of data.

8. Limitation of Liability

> Flickr shall not, under any circumstances, be liable to you for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with use of the Flickr APIS, whether based on breach of contract, breach of warranty, tort (including negligence, product liability or otherwise), or any other pecuniary loss, whether or not Flickr has been advised of the possibility of such damages. Under no circumstances shall Flickr be liable to you for any amount.

[23] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts

[24] The wording in the proposal of Directive on digital content (see note15) is ambiguous: This Directive should apply only to contracts where the supplier requests and the consumer actively provides data, such as name and e-mail address or photos, directly or indirectly to the supplier for example through individual registration or on the basis of a contract which

point it would appear that all the normal rules on performance/non-performance should apply. On the other hand, in ordinary contracts, liability of the receiving party does not change whether it has been paid in cash, precious metal, government bonds, or simply off-setting an existing debt.[25]

What if the user cannot qualify as a 'consumer' according to general EU law?[26] In the first place one should note that in the field of telecommunication services EU directives make no difference between the statuses of users. This means that rights and guarantees vis-à-vis the telecom operator apply to both 'consumers' and 'non-consumers' (typically, enterprises).[27]

Clearly this is an express normative provision, but the result is that telecom operators are burdened by a higher level of liability than over-the-top (OTT) service providers.

If this is a remark *de lege ferenda*, *de lege lata* one has to investigate – jurisdiction by jurisdiction[28] – if the exoneration clauses are valid towards non-consumer users. In some jurisdictions, clauses which limit liability require a specific form to be valid (written, express approval, etc.)[29]. In other jurisdictions – mostly of common law – one could apply the broad

allows access to consumers' photos.
This Directive should not apply to situations where the supplier collects data necessary for the digital content to function in conformity with the contract, for example geographical location where necessary for a mobile application to function properly, or for the sole purpose of meeting legal requirements, for instance where the registration of the consumer is required for security and identification purposes by applicable laws' (recital 14, emphasis added). Can one assume that in all these cases there is a contract of services, but only some of them fall under the proposed Directive?

[25] A useful test could be the Kaspersky 'Data as currency' experiment: see <https://www.kaspersky.com/blog/data-dollar-store/19660/> (accessed on Mar. 19, 2018).

[26] I.e., to use the EU template 'any natural person who is acting for purposes which are outside his trade, business or profession'.

[27] See Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, in particular the provisions concerning minimum quality standards of service.

[28] Which? If the jurisdiction clauses in the General Terms of Service of the various providers are valid one is faced with a jolly pilgrimage among the Spanish churches and convents that are scattered across California and from which its counties have taken their names: San Mateo for Facebook; Santa Clara for Google and Flickr; San Francisco for Twitter. Instagram's Terms of Use impose an arbitration clause, entirely void under EU law and, in general, in the domestic law of its Member States.

[29] E.g., the Italian Civil Code (art. 1341) requires express and written approval of a list of unfair terms, among which are included arbitration clauses and choice of a forum which is not the ordinary one.

and never clearly defined notion of unconscionability[30]. At any rate, at the end of the day, it will be up to the courts to decide whether such clauses are to be considered valid or void, and an academic lawyer's imagination is positively shallow if compared with that of judges.

4. *Non-Contractual Remedies*

The way in which loss of data may fall outside the scope of a contractual relation are countless: a careless act makes a hand-set fall in the deep blue sea; a sudden interruption of electric power (like in the classical 'cable cases'[31]) destroys a file while one is working on it; a virus infection transferred by an unsuspecting third party prevents access to a database. One can assume that there has been negligence and that the result is the definite and non-restorable loss of data. Here the initial problems will arise. In a civilian context are data an asset that belongs to the person's patrimony? Does the person that has suffered the damage hold a recognized right over such data, or does he/she simply have a right to use the data and to prevent others from using them?

Extra-contractual remedies generally protect property from negligent damage brought by third parties. But, again, is data 'property'? Once, on the basis of arguments that here are shared[32], one has excluded this approach, must one necessarily come to the conclusion that loss of data is simply one of the many cases of pure economic loss, and therefore does not give rise to compensation? Again the answer depends on how the case is presented: clearly, if the claim is that loss of data has brought business activities to a stand-still, the previously cited 'cable-cases'[33] will apply. But if the damage is related to some essential, albeit immaterial, component of the business activity, which hypothetically might even be a valuable asset

[30] E.g., s 2-302 of the Uniform Commercial Code.

[31] The comparative reference is to the English case *Spartan Steel & Alloys Ltd v Martin & Co (Contractors) Ltd* [1973] QB 27 (no damages allowed); and to the Italian case *Pasta Puddu* (Cass., Sez. unite, 24 giugno 1972 n. 2135) (damages allowed). The various German cable cases reported and commented by B. S. Markesinis, *The German Law of Torts*, (3rd edn), Clarendon, 1994, pp. 173 ff. open further perspectives: as the result of the loss of data an enterprise is forced to a standstill. Would this damage be compensated? According to the English and German precedents, the answer is negative.

[32] See the authors cited at note 3.

[33] See note 31.

in the balance sheet, one could imagine to extend to the lost database the protection already granted to other non-tangible assets such as goodwill or credit-worthiness.

There are many indicia that suggest that loss of data could be considered akin to the destruction of any valuable asset in the possession of the damaged party. The first and foremost is that willful destruction of data is, according to the Budapest Convention, a crime[34]. This allows the inference that data are a protected entity, and therefore that negligent acts – which determine the loss of data – should be subject to civil liability.

The second element that should be considered is that if personal data are qualified – as mainstream legal doctrine holds in many continental legal systems – as personality rights there is no reason to afford them less protection that other intangible situations (name, image, reputation, etc.). And even if personal data is not qualified as a personality right, it is a fundamental right under article 8 of the European Charter of Fundamental Rights.

Again it will be up to the courts – which in continental Europe and in the US (but not in the UK) have always made an expansive use of extra-contractual liability as the means to establish 'new' rights (literally, remedies have preceded rights). However, at this stage it is still unclear what the arguments for and the consequences of civil liability for the loss of data (or for the loss of access to data) will be.

5. *The Case of Loss of Personal Data*

One must consider that among the most common cases of data losses there are, and will be, the loss of personal data. The topic is amply considered in the General Data Protection Regulation[35] which applies

[34] Council of Europe, Convention on Cybercrime (Budapest, 23.11.2001):

> Article 4 (Data interference)
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

See also recital 149 of the GDPR (note 35 below): 'Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation.'

[35] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

from May 2018 onwards.

The GDPR qualifies data loss as personal data breach which entails liability on behalf of the controller or processor[36] who is burdened with an obligation to ensure an appropriate level of security[37], to inform the data subject (article 34) and to make good the person who has suffered damage[38].

From a practical point one can easily imagine that natural persons will prefer to bring their claim on the basis of such explicit norms, rather than engaging in academic qualifications on the notion of data and of their legal relevance. In such a manner also the loss of data which, *in abstracto*, could be considered not to be 'personal data' (typically when an individual collects statistics, news reports, data and information in the public domain that do not concern him/herself), will be encompassed in the GDPR provisions.

As the GDPR protects natural persons this leaves open the issue of the loss of data which 'belong' to a legal entity.

6. *Evidence*

Anybody familiar with the case-law in liability for loss of valuable objects deposited in a bank's vault or in the hotel safe is aware of the difficulty of providing evidence of what was actually lost (generally, stolen). The depositee fears that the depositor is adding into the list of stolen items

[36] Art 4 (Definitions), n. 12: '"personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

[37] Art 32 (Security of processing)

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

[38] Art 82 (Right to compensation and liability)

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

objects that were never actually deposited. Both parties face a *probatio diabolica*: should the depositor have kept a register, with witnesses of what he/she deposited? Should the depositee be able to control that what has been declared is truthful?

This dilemma – which is generally solved through burden-of-the-proof rules[39] – presents itself paradoxically when it comes to data losses. If one had to prove what data has actually been lost, that data would be in the availability of the owner, and therefore there would be no loss. To prove that the manuscript of the volume 'Research Handbook on Data Science and Law' has been lost as a result of the negligence of the digital service provider or of a third party can one limit oneself to indicate, if the log book is accessible, the number of bytes the file contained? When a business loses thousands of contacts how can it prove how many they were, how updated they were, the frequency of exchange with each contact, etc.? And the bigger the database that has been lost, the more complex is the reconstruction of its precise features: what exactly did it contain? How many entities were included? What is the nature of the meta-data?

7. Quantum *of Damages*

Although we live in a world dominated by data, in which data are considered an essential element of economy and of wealth (the 'new oil' according to certain rhetorical literature)[40] it is still quite uncertain what the actual value of data is, and if in reality the wealth is not in the (big) data itself, but rather in the computational tools (data analytics) used to extract valuable information from it. One has precise market prices for profiles of individuals used for marketing (especially in the medical sector)[41], but very

[39] The typical English response is that there is no evidence: see *Andre & Anor v Clydesdale Bank Plc* [2013] EWHC 169 (Ch). At the opposite the Italian Corte di Cassazione states that one can prove the content through simple presumptions and witnesses: see for the latest in long line of decisions Cassazione civile, sez. I, 27.7.2017, n. 18637.

[40] Ex multis, *The Economist*, May 6, 2017 'The world's most valuable resource is no longer oil, but data' <https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worldsmost-valuable-resource> (accessed on Mar. 19, 2018). Illustrated with a picture of the main data companies (Google, Facebook, etc.) rigging in a sea of data.

[41] See the US Senate Report on 'A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes' available at <https://www.commerce.senate.gov/public/index.cfm/reports?ID=57C428EC-8F20-44EEBFB8-A570E-

little evidence on how much a database of clients is worth in a business transaction[42]; or what is the overall cost to re-build a lost directory[43]. If this is valid for business entities, even more difficulties can be encountered when the loss concerns personal correspondence, addresses, photographs, videos. How to evaluate the damage from the loss of hundreds of love messages, an archive of family snap-shots, etc.? One can imagine applying rule-of-thumb criteria common for non-patrimonial losses, but this leaves a very wide area of discretion, in which the position of the defendant service provider is greatly advantaged in the countries (i.e., all, except the US) where no punitive damages are awarded[44].

9BE0CCC> (accessed on Mar. 19, 2018) or the US FTC Report 'Data Brokers. A Call for Transparency and Accountability' available at <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf> (accessed on Mar. 19, 2018). For a European attempt to establish the value of data see the Report by the Italian Telecoms Regulatory Agency (AGCOM), Big data. Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS (available at https://www.agcom.it/documents/10179/10875949/Studio-Ricerca+08-06-2018/c72b5230-354d-444f-9e3f-5467ca450714?version=1.0)

[42] Uncertainty is reflected in the articles concerning this topic: see D. Borelli, *International Trading of Big Data*, in Athens Journal of Law, vol. 3, 21, 2017, p. 26 ff; P. Waelbroeck, *The Economic Value of Personal Data: An Introduction* (October 2015), available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2690109> (accessed Mar. 19, 2018). Some indications could be drawn from the US Radio Shack bankruptcy case in which over 100 million of data concerning former clients were put on sale, but encountered considerable privacy issues (for a few news reports see <https://www.law360.com/articles/679550/customer-data-sale-in-bankruptcy-lessons-from-radioshack> (accessed on Mar. 19, 2018) or <http://www.infolawgroup.com/2015/06/articles/privacy-law/radioshackbankruptcy-case-highlights-value-of-consumer-data/> (accessed on Mar. 19, 2018).

[43] Useful indications come from the German BGH decision 9.12.2008 (VI ZR 173/07) which struck down the decision of the court of appeal which had awarded only the cost of new memory disk, stating that the damaged suffered was the cost necessary to recreate the database.

[44] One could imagine that in many cases the courts might consider that the damage is trivial, and not worth compensation according to the *de minimis non curat praetor maxim*. Some indications in this sense come from the Italian Court Cassation in cases in which individuals had claimed damages for the violation of the rules concerning the processing of personal data: in Cass. 13.10.2016, n. 20615 the claim for damages following the publication of personal data within a document of a municipality on its website was rejected. In Cass. 8.2.2017, n.3311 the request of damages for € 360 for having received ten unsolicited mails was considered 'hypothetic, futile, consisting, at most, in a modest inconvenience or discomfort, which could have been surely tolerated'. The claimant was sentenced to pay € 1500 for abuse of judicial process. The attempt to join actions

This reasonable forecast suggests that from a policy perspective compensation schemes should be introduced. One can easily expect that in most cases the data loss will be a 'mass loss', in the sense that some break-down of the system or some external breach will determine the loss of data pertaining to hundreds, thousands or even millions of individuals or entities.

In these cases ordinary judicial remedies (both contractual and noncontractual) are quite ineffective also because of the very high administrative and legal costs.

Much more efficient – *de lege ferenda* – is a system in which compulsory insurance for data service providers is supplemented by simplified and semi-automatic compensation procedures, similar – although on a larger scale – to those one already finds in the EU transport law for the protection of passengers[45].

To conclude: data losses, as many other aspects concerning data societies and data economies, still lie in uncharted waters. The notion itself of data and its legal classification is debatable, at least among jurists. But also other sciences – noticeably economic – do not yet provide certain and agreed bearings. Only the combined efforts of academic research, advised regulators and competent courts can slowly open the way to a more precise and reliable setting.

throughout Europe for misuse of personal data using Regulation 44/2001 was rejected by the CJEU in the Schrems II decision (Case C-498/16, decided 25.1.2018).

[45] See Regulation (EC) No 261/2004 of the European Parliament and of the Council of 11 February 2004 establishing common rules on compensation and assistance to passengers in the event of denied boarding and of cancellation or long delay of flights, and repealing Regulation (EEC) No 295/91; Regulation (EC) No 2027/97 of 9 October 1997 on air carrier liability in respect of the carriage of passengers and their baggage by air; Regulation (EC) No 1371/2007 of the European Parliament and of the Council of 23 October 2007 on rail passengers' rights and obligations; Regulation (EU) No 1177/2010 of the European Parliament and of the Council of 24 November 2010 concerning the rights of passengers when travelling by sea and inland waterway; Regulation (EU) No 181/2011 of the European Parliament and of the Council of 16 February 2011 concerning the rights of passengers in bus and coach transport.

Vincenzo Zeno-Zencovich

Free-Flow of Data: Is International Trade Law the Appropriate Answer?

1. *Introduction: The Problem*

The free-flow of data (FFD) is a major concern in international political and economic relations. In the last decade, there have been growing signs of 'data nationalism'[1] and of 'data balkanization'.[2] The normative formalisation of such trend is very well represented by Article 3 of EU Regulation 2016/679, the General Data Protection Regulation (GDPR)[3] according to which:

> 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
> 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>   a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>   b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

---

* This article was first published in *Data Protection Beyond Borders. Transatlantic Perspectives on Extraterritoriality and Sovereignty*, F. Fabbrini, E. Celeste, J. Quinn (eds.), 2020, pp. 173-188.

[1] A. Chander and U. P. Lê, *Data Nationalism*, in *Emory Law Journal*, vol. 64, 2015, 677.

[2] J. Daskal, The *Un-Territoriality of Data*, in *Yale Law Journal*, vol. 125, 326, 2015: 'Balkanization of the Internet into multiple, closed-off systems protected from the exterritorial reach of foreign-based ISPs', p. 332.

[3] For a thorough analysis of the issue I will simply refer to the chapters in this volume by Federico Fabbrini and Edoardo Celeste (Ch 2), and by Oreste Pollicino (Ch 6). Previously see S. J. Schulhofer, *A Transatlantic Privacy Pact ? : A Sceptical View*, and D. Cole, F. Fabbrini , *Transatlantic Negotiations for Transatlantic Rights: Why an EU-US Agreement is the Best Option for Protecting Privacy against Cross-border Surveillance*, both in D. Cole, F. Fabbrini, S. Schulhofer (eds), *Surveillance, Privacy and Trans-Atlantic Relations* (Hart Publishing, 2017).

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

The extremely wide territorial scope of the Regulation is justified by the statement that 'the processing of personal data should be designed to serve mankind' (Recital 4) and that '[t]he principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data' (Recital 2)[4].

The USA quickly responded to such stance – also to counter attempts by US firms to place their data outside the domestic territory and jurisdiction – through its 2018 CLOUD Act[5], which in its recitals states:

Congress finds the following:

(1) Timely access to electronic data held by communications-service providers is an essential component of government efforts to protect public safety and combat serious crime, including terrorism.

(2) Such efforts by the United States Government are being impeded by the inability to access data stored outside the United States that is in the custody,

[4] One can find the idea of an EU sovereignty in the field of data protection already in the CJEU decision in the USA-EU PNR controversies (Joined cases C-317/04 and C-318/04 European Parliament v Council of the European Union and European Parliament v Commission of the European Communities, decided on 30 May 2006, ECLI:EU:C:2006:346). However, the first formal declaration of EU data sovereignty is in the *Schrems* decision, widely commented on in this volume. With permission I would refer to V. Zeno-Zencovich, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, 2015, 31 (4–5) Il diritto dell'informazione e dell'informatica 683 , and to the copious literature cited therein. The English version of the article *Around the CJEU Schrems Decision: Digital Sovereignty and International Governance of Telecommunication Networks* is available at: SSRN papers.ssrn.com/sol3/papers.cfm ? abstract_id=2788789. Only a few days before this chapter was sent to the publisher the CJEU rendered its decision in the *Schrems III* case C-311/18) declaring the so-called ' Privacy Shield ' agreement between the EU and the US invalid. It is impossible to analyse the extremely lengthy (50 pages) decision by the Grand Chamber. Suffice it to point out that the gist of the case is the transfer of personal data outside the territory of the EU and the renewed affirmation of EU sovereignty over personal data collected in Europe. The implications of the decision for international economic (and political) relations can be seen in the light of the arguments set out in this chapter, without forgetting (and adapting) JH von Kirchmann's 1847 famous quote from his Berlin lecture on *The Worthlessness of Jurisprudence as a Science*: 'Three lines from the Court of Justice and entire libraries become waste paper'.

[5] HR 4943 – Clarifying Lawful Overseas Use of Data Act (CLOUD Act) (available at the US Congress website: <http://www.congress.gov/bill/115th-congress/house-bill/4943>).

control, or possession of communications-service providers that are subject to jurisdiction of the United States.
(3) Foreign governments also increasingly seek access to electronic data held by communications-service providers in the United States for the purpose of combating serious crime.
(4) Communications-service providers face potential conflicting legal obligations when a foreign government orders production of electronic data that United States law may prohibit providers from disclosing.
(5) Foreign law may create similarly conflicting legal obligations when chapter 121 of title 18, United States Code (commonly known as the 'Stored Communications Act'), requires disclosure of electronic data that foreign law prohibits communications-service providers from disclosing.
(6) International agreements provide a mechanism for resolving these potential conflicting legal obligations where the United States and the relevant foreign government share a common commitment to the rule of law and the protection of privacy and civil liberties.

And the Act's first and foremost provision – § 2713 – determines unambiguously:

> A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.

Although the preambles of the US Act and a subsequent decision of the EU Court of Justice (*Google v CNIL*)[6] declare that the aim of the two normative provisions is that of avoiding conflicts of laws, the practical result is that the same database may be subject to conflicting jurisdictions. At any rate the conflict is deeply rooted in the different views of the main international actors – EU, USA, and China – on international relations and on the role that data flows play in geopolitical strategies[7].

Over these last years there have been growing concerns on the effects, present and future, of such conflicts, and legal scholarship has often indicated that the appropriate legal and institutional context in which to solve them is that of international trade and of global or regional trade law and

[6] Analysed in this volume by John Quinn, Ch 4.
[7] See H. Choer Moraes, *The Geoeconomic Challenge to International Economic Law: Lessons from the Regulation of Data in China* (available on SSRN at: papers.ssrn.com/sol3/papers.cfm?abstract_id=3479504) who speaks of a 'clash of models'.

negotiated agreements[8].

[8] The literature from the international trade law perspective has considerably grown in these last years. For a first selection, without any pretence of completeness, see: S. A. Aaronson and P. Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, in *Journal of International Economic Law* 245, 2018; I. Brannon and H. Schwartz, *The New Perils of Data Localization Rules*, in *Regulation* vol. 41(2), 12, 2018; M. Burri, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, in *UC Davis Law Review*, vol. 51, 65, 2017; C-M Chung, *Data Localization: The Causes, Evolving International Regimes and Korean Practices*, in *Journal of World Trade*, vol. 52, 187, 2018; D. Ciuriak, M. Ptashkina, *Towards a Robust Architecture for the Regulation of Data and Digital Trade*, (July 2019) available on SSRN at: papers.ssrn.com/sol3/papers.cfm?abstract_id=3423394; B. Cohen, B. Hall and C. Wood, in *Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy*, in *Antitrust*, vol. 32, 107, 2017; A. Coley, *International Data Transfers: The Effect of Divergent Cultural Views in Privacy Causes Déjà vu*, in *Hastings Law Journal*, vol. 68, 1111, 2017; V. Conrad, *Digital Gold: Cybersecurity Regulations and Establishing the Free Trade of Big Data*, in *William & Mary Business Law Review*, vol. 10, 295, 2018; M. A. Corley, *The Need for an International Convention on Data Privacy: Taking a Cue from the CISG*, in *Brook Journal of International Law*, vol. 41, 721, 2016; H. Gao, *Digital or Trade? The Contrasting Approaches of China and US to Digital Trade*, in *Journal of International Economic Law*, vol. 21, 297, 2018; S. Hodson, *Applying WTO and FTA Disciplines to Data Localization Measures*, in *World Trade Review*, vol. 18, 579, 2019; J. Kelsey, *How a TPP-Style E-commerce Outcome in the WTO would Endanger the Development Dimension of the GATS Acquis (and Potentially the WTO)*, in *Journal of International Economic Law* , vol. 21, 273, 2018; J. P. Meltzer, *A New Digital Trade Agenda, Overview paper of the E15 Expert Group on the Digital Economy* (August 2015) (available on-line at: <http://www.e15initiative.org/wp-content/uploads/2015/07/E15-Digital-Economy-Meltzer-Overview-FINAL.pdf>); A. D. Mitchell and N. Mishra, *Data at the Docks: Modernizing International Trade Law for the Digital Economy*, in *Vanderbilt Journal of Entertainment & Technology Law*, vol. 20, 1073, 2018; A. D. Mitchell and N. Mishra, *Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute*, in *Journal of International Economic Law*, vol. 22, 389, 2019; S. Peng and H. Liu, *The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help*, in *Journal of World Trade*, vol. 51, 183, 2017; J. Pumr, *Digital Platforms as Big Data Harvesters in the Digital Economy – Competition Overview*, in *Common Law Review*, vol. 16, 40, 2020; J. Selby, *Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both*, in *International Journal of Law & Information Technology*, vol. 25, 213, 2017; N. Sen, *Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?, in Journal of International Economic Law*, vol. 21, 323, 2018; J. Thierer, *Privacy as an Obstacle: Data Privacy Laws under the GATS*, in *Freilaw: Freiburg Law Students Journal*, 2018, 8; B. Wong, *Data Localization and ASEAN Economic Community*, in *Asian Journal of International Law*, vol. 10, 158, 2020; S. Yakovleva, *Should Fundamental Rights to Privacy and Data Protection Be a Part of the EU ' s International Trade Deals ?*, in *World Trade Review*, vol. 17, 477, 2018; S. Yakovleva and K. Irion, *The Best of Both Worlds ? Free Trade in Services, and EU Law on Privacy and Data Protection*, in *European Data Protection Law Review*, 191, 2016 (available on SSRN at: papers.ssrn.com/sol3/papers.cfm

In this direction there are already several examples which are commonly indicated as models. In this chapter, I will attempt to highlight that although certain world or multilateral trade institutions (eg the WTO or the OECD) may be the most productive through which to work out accepted and effective solutions, the basic principles of international trade that have been elaborated over the last 75 years are not generally applicable to FFD because of certain unique features which require different approaches and solutions.

As such, the chapter is structured as follows: I will first analyse FFD from the point of view of general and regional international trade law agreements. I will then critically evaluate their application to the extremely vast – if not fuzzy – notion of 'data' and the possibility that it may be the object of 'trade'. I then present the argument that the 'Most Favoured Nation' (MFN) and 'National Treatment' (NT) principles appear impracticable when applied to data. I conclude with some suggestions of tentative solutions and on the fora where they could be reached.

2. *The International Trade Frame of Reference*

If one tries to set a few firm points in the debate on the free-flow of data, one must necessarily consider, in the first place, decisions taken in the WTO and regional agreements context.

This appears reasonable: data are essential for economic activities, both to record the present and the past of contractual relations, and to understand and forecast the future.

However, in an 'Industry 4.0' context, data is collected for a multiplicity of other reasons, mainly to monitor constantly one's devices and to collect surrounding information. At any rate, we are quite often confronted with a constant and uninterrupted flow of data. Halting it prevents the functioning of analytics based on real-time input and immediate response (e.g. data from the 'black box' of an automobile).

Therefore, one can easily detect a few loopholes, with the first being that generally, data flows are not the object of an international trade transaction (goods bought or sold; services requested or provided), but are ancillary

?abstract_id=2877168); P. K Yu, *Data Exclusivities and the Limits to Trips Harmonization*, in *Florida State University Law Review*, vol. 46, 641, 2019. One can refer also to the special issue of *Digital Policy, Regulation and Governance*, vol. 21, 2019, devoted to *Digital Trade vs Cyber Nationalism*.

aspects of any economic activity, in the sense that enterprises have always collected data on their clients and providers and on the contracts they have with them.

The second, and consequential, problem is that data flows are not easily classifiable as goods or services, and therefore there is uncertainty whether they fall under the General Agreement on Tariffs and Trade (GATT) or under the General Agreement on Trade in Services (GATS)[9]. Could one claim that the first applies when the core business is the trade of goods; the second, when the core business in the provision of services? Or is this a case of international barter (or countertrade)?[10]

Further, in many online services, data (personal and metadata) are the consideration for the services provided. Can one apply to this flow the provisions which can be found in international trade treaties or in the IMF Agreement which regulate restrictions on payments and currency exports?[11]

Some provisions are even more specific and are generally cited by the literature on the issue:

a) The 1997 Annex to the WTO Protocol on market access to basic telecommunications states (§ 5) that members are granted access to and use of public telecommunications networks on non-discriminatory terms for the supply of various services including 'data transmission, typically involving the real-time transmission of customer-supplied information between two or more points'.

[9] M. Ferracane, *Data Flows and National Security: A Conceptual Framework to Assess Restrictions on Data Flows under GATS Security Exception*, in *Digital Policy, Regulation and Governance*, vol. 21, 44, 2019, simulates a WTO dispute on data flow restrictions. One has, however, to point out that while GATT has been an overall success for international trade of industrial products, GATS has substantially failed in its objectives for the reasons clearly and authoritatively set out by M. J. Trebilcock, *International Trade Law*, Edward Elgar, 2015, who points out (see section III below) the extreme difficulty of applying the MFN and NT principles to trade in services, pp. 125 ff. Also, in the framework of GATS – highlighting several stumbling blocks – see A. D. Mitchell and N. Mishra, *Data at the Docks: Modernizing International Trade Law for the Digital Economy*, *supra* note 8.

[10] See V. de Beaufort, E. Devilder and C. Sylvain, *Competitiveness of European Companies and International Economic Countertrade Practices*, in *International Business Law Journal* 1, 2014; or R. Howse, *Beyond the Countertrade Taboo: Why the WTO Should Take Another Look at Barter and Countertrade*, in *University of Toronto Law Journal*, vol. 60, 289, 2010. UNCITRAL in 1993 issued a *Legal Guide on International Countertrade Transactions*. From an economic perspective see also D. Marin, M. Schnitzer (eds), *Contracts in Trade and Transition. Th e Resurgence of Barter*, MIT Press, 2002.

[11] See Article VIII, § 2(a) of the IMF Articles of Agreement: 'no member shall, without the approval of the Fund, impose restrictions on the making of payments and transfers for current international transactions.'

b) The same provision states (letter c) that service suppliers may use telecommunication networks for the movement of information within and across borders and for the access to information contained in databases.
c) However (letter d), members may take measures 'to ensure the security and confidentiality of messages' provided this does not constitute a means of unjustifiable discrimination or a 'disguised restriction on trade in services'[12].

The provisions in the WTO Telecommunications Annex are substantially repeated in Chapters 13 and 14 of the ' Comprehensive and Progressive Agreement for Trans-Pacific Partnership', which replaced the original Trans-Pacific Partnership Agreement after the USA withdrew its signature in 2017. In particular, Article 14.13 of the Agreement, under the heading ' Location of Computing Facilities' states that:

1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.
2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory[13].

At a regional level one can mention the Asia-Pacific Economic Cooperation (APEC) and the Cross-Border Privacy Rules (CBPR) System[14]. Although the guidelines are not binding, they provide useful indications on how to balance the different interests i.e. on the one hand protecting personal information from misuse and unwanted intrusions; on the other hand, enabling global organisations to collect, access, use and process data

[12] In a 2004 paper, K. Bressie, M. Kende and H. Williams, *Telecommunications trade liberalization and the WTO*, available on-line at: <http://www.hwglaw.com/wp-content/uploads/2004/09/69A7C2994A9A82580D112146E5FB0E0C.pdf>, express the view that 'WTO commitments act to stimulate foreign investment in the sector by opening up the market, acting as a credible commitment to reforming the domestic telecommunications sector and providing recourse to foreign investors through the World Trade Organization's dispute resolution system'. Reviewed after 15 years, the optimistic outlook does not appear to have been confirmed.

[13] S. Hodson, *Applying WTO and FTA Disciplines to Data Localization Measures*, *supra* at note 8, sees the CPTPP as a significant improvement in respect of GATS.

[14] The current text (updated as of November 2019) states in its preambles that 'APEC plays a critical role in the Asia Pacific region by promoting a policy framework designed to ensure the continued free flow of personal information across borders while establishing meaningful protection for the privacy and security of personal information'.

in the member countries. The system is based on four steps: (*i*). self-assessment by organisations engaged in cross-border flow of data; (*ii*). compliance review by APEC; (*iii*). recognition, acceptance and listing in a compliance directory; and (*iv*). procedures for enforcement and dispute resolution.

The 2019 US-Mexico-Canada Trade Agreement (USMCA), which has (partially) replaced the North American Free Trade Agreement (NAFTA) among the same three countries, devotes Chapter 19 to 'Digital Trade'[15] and explicitly refers to the APEC-CBPR, with some important specifications – such as designating restrictive measures based on policy objectives as not compliant if they are 'at the detriment of service suppliers of another Party' (Article 19.11, note 5). The Agreement replicates in Article

[15] 'Article 19.8: Personal Information Protection

1. The Parties recognize the economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade.
2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. In the development of this legal framework, each Party should take into account principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013).
3. The Parties recognize that pursuant to paragraph 2, key principles include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability. The Parties also recognize the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented.
4. Each Party shall endeavor to adopt non-discriminatory practices in protecting users of digital trade from personal information protection violations occurring within its jurisdiction.
5. Each Party shall publish information on the personal information protections it provides to users of digital trade, including how:
   (a) a natural person can pursue a remedy; and
   (b) an enterprise can comply with legal requirements.
6. Recognizing that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. Th e Parties shall endeavor to exchange information on the mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them. Th e Parties recognize that the APEC Cross-Border Privacy Rules system is a valid mechanism to facilitate cross-border information transfers while protecting personal information.'

19.12 and under the same heading the provision one has already seen in the 'Comprehensive and Progressive Agreement': 'No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.'

Another text that should be considered is the EU-Canada Comprehensive Economic and Trade Agreement (CETA), which contains numerous provisions concerning cross-border flow of information in terms not dissimilar to those that have been indicated above[16].

3. *A Critical Appraisal of the International Trade Approach*

The first necessary remark is that 'data' (and therefore FFD) is an extremely vague notion which can be filled with many – and not necessarily consistent – meanings[17]. But the first, and preliminary, objection is that in a digital environment everything is 'data', and 'data' is produced, collected, processed and delivered through telecommunication networks. Any present-day communication – whether for personal, professional, commercial, institutional, cultural purposes – is made through the transmission and

[16] Eg Article 13.15 on 'Transfer and processing of information': '1. Each Party shall permit a financial institution or a cross-border financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing if processing is required in the ordinary course of business of the financial institution or the cross-border financial service supplier. 2. Each Party shall maintain adequate safeguards to protect privacy, in particular with regard to the transfer of personal information. If the transfer of financial information involves personal information, such transfers should be in accordance with the legislation governing the protection of personal information of the territory of the Party where the transfer has originated'.
Or Article 15.3, at para 3: 'Each Party shall ensure that enterprises of the other Party may use public telecommunications transport networks and services for the movement of information in its territory or across its borders, including for intra-corporate communications of these enterprises, and for access to information contained in data bases or otherwise stored in machine-readable form in the territory of either Part'. This is a template one finds replicated in the recent (June 2020) *Free trade agreement between the European Union and the Socialist Republic of Viet Nam*.

[17] On the distinction between data in motion, data at rest and metadata, see T. Maurer et al, *Technological Sovereignty: Missing the Point?*, in M. Maybaum, A-M Osula and L. Lindstrom (eds), 2015 7th International Conference on Cyber Conflict: Architechtures in Cyberspace (NATO CCD COE Publications, 2015) at p. 56 [available on-line at: ccdcoe.org/sites/default/files/multimedia/pdf/Art%2004%20Technological%20Sovereignity%20-%20Missing%20the%20Point.pdf].

reception of data. From this perspective, it would appear that FFD has to do much more with the general fundamental right of communication guaranteed by the UN Charter and by the 1969 New York Covenant on Civil and Political Rights, than with international trade. The interaction between these two spheres is widely discussed and very good reasons have been set out to keep them separated if one does not wish to jeopardise international trade relations. At any rate, this requires distinguishing – a difficult process as we shall see – between the different kinds of 'data' and their actual inherence with international trade. The question of FFD brings us thus to establish, what 'data' are we concerned with?

This raises the question if it is possible to distinguish between 'aggregated' data, which provides an overall view of a certain situation at a certain time (or over a certain period); and 'granular' data which enables us to understand the situation of a particular natural person or of a legal entity.

The former appears to be less problematic if and when such aggregated data are held and made available by public institutions (typically those in charge of national statistics). The latter instead raises concerns not only for the protection of personal data issues, but also because such granular data are quite often collected in real time and allow for a constant monitoring of what is going on (a financial crisis, a sanitary epidemic, etc) in a different country. This has very little to do with international trade and very much with geo-politics and diplomatic relations.

A further related issue is that of 'trade'. When we talk about FFD are we considering 'data' as a commodity which is collected or delivered across borders? Or is data an ancillary aspect of any transaction? If the latter is free, the former should also be. Or is data the consideration for services that are rendered through digital networks?

This requires distinguishing between the many uses and purposes of 'data'.

Firstly, in any economic transaction the parties collect data on the performance of the transaction, on the counterpart, and on other surrounding circumstances. For example, in the sale of machinery or in the opening of a line of credit, it is obvious that this data flows together with the core of the transaction, which cannot stand without the parties receiving, communicating and processing such data.

To use a Latin expression, such flows are *naturalia negotia*, and therefore there is no need to change existing trade agreements and practices.

A different problem arises when data flows within the same entity or a group of entities. The typical example is that of the sales of a foreign

subsidiary or the information concerning employees belonging to the same multinational group. As we have seen, there are relevant normative provisions that allow this, but again it does not raise significant doubts and appears to be an inherent aspect of international trade.

Much more to the point is when the collection of data is the core business of the enterprise (as in search engines or social media platforms). In these cases, there is a service which is provided without any monetary payment but in exchange for personal and non-personal data, and therefore there is a genuine international trade issue which concerns the freedom to provide services and the limitations which may be attached. One should note that in these cases the concern is not so much about the nature of the service provided, but about the counterparty: the users from and through whom data is collected. If the service were paid for with a monetary compensation there would hardly be a problem, in the sense that it would be considered like any other contract for the provision of services. The fact that data – both personal and non-personal – are involved creates the political and economic concerns which have been presented at the beginning of this chapter and which need to be tackled in this section.

However, there are many activities in which the collection and processing of data is an important aspect of the goods or of the services provided. The obvious examples are given by the data collected by the 'black box' of a car and transferred to the producer, or the data collected by online hotel or plane reservation platforms. In general, all the Internet-of-Things (IoT) devices collect data during their functioning, whether in a house (domotics) or in an urban context (smart cities) or in a business organisation (Industry 4.0). Clearly, restrictions to FFD amount to the restriction of the international trade of those goods or services.

The EU approach, which is followed in other countries, is that of establishing limitations concerning 'personal data' , i.e. data which is directly or indirectly referable to an individual. The best example is Regulation 2018/1807 'on a framework for the free flow of non-personal data in the European Union', which should have been fully implemented by May 2020. According to such legislation, '"data" means data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679' (i.e. the GDPR). This classification is however rather unrealistic. When any entity (a private individual, a business entity, an organisation, a public entity) collects data, it is quite impossible to distinguish between 'personal' data and ' non-personal ' data because data describe complex situations that have a common link. In the simple data concerning the sale of an

object that must be delivered, one has a name: that of the buyer, but also the data concerning the object sold, the address, the carrier, the route etc. Furthermore, there is a fundamental misunderstanding when the GDPR builds its system on 'personal' data, imagining that the data belongs to one and only one 'data holder'. Generally, most of the data individuals generate are relational, in the sense that they express a relationship between two or more individuals or entities. In a contract it makes little sense stating that one party has some kind of entitlement over 'its' data, and the other party over 'its' data. All the data is shared and belongs (in an a-technical sense) to all the parties in the relationship. If one reconstructs the relationship between user and provider of on-line digital services (e.g. a search engine) as a contract (services in exchange of data), it is clear that the 'personal data' provided by the individual and all the metadata belong to both parties. Furthermore, the procedures to anonymise data in such a way that it is impossible to trace back the natural person to which it is referable are complex and uncertain in their result, in the sense that existing programs are able to reverse the process leading to the identification of the subject.

As has already been mentioned, the relationship between international trade law and fundamental human rights is highly problematic. On the one hand, one can point out that developed economies cannot ignore the political, economic and social plight of the countries with which they trade. These developed economies are taking advantage and are exploiting the poverty, not only economic, of millions of individuals. On the other side, one is reminded (since Smith and Ricardo) that international trade thrives on such differences – especially on the difference in the cost of labour and on comparative advantages – and behind the human rights stance there are strong protectionist pressures which result in leaving the poor even more poor.

But in the case of personal data the main issue is not that of ensuring that people living in distant countries are granted an acceptable level of protection that is considered a human right in the West. One therefore, is not talking of (authentic or pretended) 'bad conscience' of producers and consumers in developed countries. The issue is that of avoiding that fundamental rights that are already recognised and guaranteed are jeopardised by international trade and its freedom.

FFD becomes therefore a concern under two novel aspects: firstly, allowing producers of goods and providers of services access to a jurisdiction in which personal data are protected requires a prior balancing of the trade-offs between consumer welfare and citizens' rights; secondly, it raises political and international concerns inasmuch as other countries or powerful multinational enterprises have access to and at their disposal

the informational database of the citizens of a different nation, in order to direct their international and business policies.

If one considers that the data can be extracted from a nation – not only from its citizens – as a strategic digital resource, rather than in an international trade context it would appear more appropriate to classify it as a national resource that can be exploited by foreign entities only on the basis of extremely detailed conditions, such as those that allow mining, oil extraction or off-shore platforms.

From this perspective one way out might be that of verifying the applicability of so-called countertrade practices and principles when services (telecommunications) or goods (with an embedded digital online memory) are traded in exchange for access to data.

4. *Impracticability of the MFN, NT and TBT Principles*

The argument that FFD does not properly fit within international trade is reinforced if one tries to apply the two main pillars of international trade law which have guaranteed its unparalleled success over the last 75 years.

The first is the 'Most Favoured Nation' (MFN) principle, engraved in Article I of the GATT Treaty. In substance, it means that if two countries have reached a tariff agreement on the import/export of certain products, the same treatment must be applied 'immediately and unconditionally' to like products from a third country. The provision is replicated for services, in Article II of the later GATS Treaty. The first stumbling-block is, as has already been mentioned, the dubious nature of data as a 'product' or 'service', and therefore the assimilation of FFD to the international circulation of goods and of services. Furthermore, it is rather problematic – if one gives importance to words – trying to identify 'like products' of data. More to the point is the notion of 'like services and service supplies', set in Article II of the GATS Treaty[18]. Again, FFD is not in itself a service; it is quite often an activity collateral to some other production of goods or provision of services.

However, the main obstacle to the application of the MFN principle is that, as FFD is allowed on the basis of reciprocity and of mutual concessions, the application of the MFN principle is unworkable because it would circumvent the whole system, without bringing any advantage to trade or to

[18] The 'services' approach is favoured by S. Yakovleva and K. Irion, *The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection*, supra at note 8.

international cooperation. As a matter of fact, the application of the MFN principle would be a major obstacle to agreements on free-flow of data.

The National Treatment principle does not fare well in FFD, because the concern – whether individual or national – is not how data is processed within the territory of the country, but if and how it is (or can be) processed once it is taken abroad. Therefore, the objections are raised over the external – and not the domestic – obligations that bind the data processor in its own jurisdiction.

Further, reservations have been raised over data protection laws (noticeably the GDPR) being a form of Technical Barrier to Trade (TBT), contrary to the principles set out in the Tokyo Round[19]. Again, inasmuch as data protection rules are applied in a non-discriminatory way, there appears to be no violation. The 'barrier' is not to enter the market but to export the results of the activity in the form of data. This brings us back to the notion of national informational resources and the possibility for third parties to exploit them. The provisions on 'data localisation' – which we have seen are waived in the 'Comprehensive and Progressive Agreement for Trans-Pacific Partnership ' and in the US-Mexico-Canada Trade Agreement (USMCA) – which require that data should be processed only in the country where they are collected, could be classified as TBTs[20].

5. *Some Tentative Solutions*

If traditional and well-oiled international trade law principles appear to be inadequate to tackle FFD[21], can one suggest some viable alternatives?

[19] This is among the conclusions of S. Yakovleva and K. Irion, *The Best of Both Worlds?*, *supra* note 8; see also B. Wong, *Data Localization and ASEAN Economic Community*, *supra* note 8.

[20] One could, however, express some scepticism over some economic analysis (I. Brannon and H. Schwartz, *The New Perils of Data Localization Rules*, supra note 8) which purports to predict the losses in case of a broad data-localisation obligation.

[21] Quite obviously not everybody shares the same view: see L. Chen et al, *The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies*, Policy Brief Under T20 Japan Task Force 8: Trade, Investment and Globalization, available on-line at: t20japan.org/policy-brief-digital-economy-economic-development/, according to whom ' a systematic formation of policies for the flow of data and data-related businesses can be developed based on an analogy with trade in goods. On this basis, the brief classifies a series of data-related policies based on the standard microeconomic theory, and provides a starting point for policy making'.

The points and legal references that follow are only an attempt to sketch a different path which follows – albeit with some *Realpolitik* – issues that inevitably will turn up[22].

Sovereignty. Although sovereignty is a disputed issue[23], this chapter posits that each country retains sovereignty over telecommunication networks established in its territory and holds the right to regulate the data – whether personal or not – that are produced on its territory. The starting point could be similar to that expressed in Article 1 of the 1944 Chicago Convention on civil aviation.

One may venture that one of the reasons for present-day 'data nationalism' is the uncertain status of data and consequently of FFD. The reference to civil aviation is relevant because telecommunications networks share many common features with air, sea and space activities[24], with the further

[22] Further suggestions, some similar to those here presented, some diverging, can be found in S. A. Aaronson, *Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows*, CIGI Papers No 197 – November 2018 (available on-line at: <http://www.cigionline.org/publications/data-diff erent-why-world-needs-new-approach-governing-cross-border-data-flows>). For more policy indications see N. Cory, R. D. Atkinson and D. Castro, *Principles and Policies for "Data Free Flow With Trust"*, Information Technology & Innovation Foundation Paper (27 May 2019) (available on-line at: itif.org/publications/2019/05/27/principles-and-policies-data-free-fl ow-trust) according to whom '1. The digital economy's foundation is cracking as some countries try to impose their rules on others, and some erect barriers and turn inward. 2. To maximize the innovation and productivity benefits of data, countries that support an open, rules-based trading system need to agree on core principles and common rules. 3. Rather than tell firms where they can store or process data, countries should hold firms accountable for managing data they collect, regardless of where they store or process it. 4. Countries should revise inefficient processes and outdated legal agreements governing law enforcement access to data stored in other jurisdictions. 5. Countries should adopt policies with appropriate checks and balances for ISPs to block data flows involving illegal distribution of unlicensed content. 6. For data to flow " with trust, " countries must support the key technology people and businesses rely on to ensure its confidentiality: encryption'.

[23] I have tried to present the various arguments, in favour and against, also from an international law perspective in my article *Around the CJEU Schrems decision*, *supra* note 4.

[24] It seems logical to assimilate it to the high seas, international airspace and outer space: W. Heintschel von Heinegg, *Legal Implications of Territorial Sovereignty in Cyberspace*, in C. Czosseck, R. Ottis, K. Ziolkowsky (eds), *2012 4th International Conference on Cyber Conflict*, NATO CCD COE Publications, 2012, at p. 9 [available on-line at: ccdcoe.org/sites/default/files/multimedia/pdf/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf] at p. 9; see also P. W Franzese, *Sovereignty in Cyberspace: Can It Exist?*, in *Air Force Law Review*, vol. 64, 1, 2009, at p. 40f. Th e similarity is used also to attempt to establish jurisdiction in private international law issues: see W. G. Jimenez and A. R Lodder, *Analyzing Approaches to Internet Jurisdiction Based on Model of Harbors and the High Seas*, in *International Review of*

complexity that the routes that data follow are not predetermined in transport, but can vary according to technical features, typically the congestion of the network. This raises issues on what we mean by 'transit' (guaranteed by Article V of the GATT treaty) in FFD.

It is well known that the path a communication takes through the Internet depends on a series of factors which are generally autonomous from the decision of the sender. Can one apply customary international rules on passage? Do states have a sovereign right to control (and eventually block or 'seize') communications that pass through their territory?[25]

Reciprocity. A second element that can be usefully extracted from the international transport models is that of reciprocity, which enhances mutual trust and the search for solutions that keep up with the very rapid evolution of technology, social and economic uses of data. Concessions are therefore easier to obtain and grant, promoting templates that can be easily adopted elsewhere[26].

Opt-out approach. From a procedural point of view, it would appear preferable if, instead of having to negotiate each aspect of the agreement, the parties were faced with an extremely broad template which envisages full FFD. Discussions would therefore be centred on the specific aspects that should be kept out of the agreement or should be dependent on specific conditions.

Extraterritoriality. Just like in the law of the sea one has territorial waters and the high seas, one has to imagine the data regime when the data are outside a national jurisdiction[27]. The are some indications as to networks

Law, Computers & Technology, vol. 29, 266, 2015.

[25] See W. Heintschel von Heinegg, *Legal Implications of Territorial Sovereignty in Cyberspace*, *supra* note 24, who suggests that this might be restricted on the basis of 'customary or conventional rules of international law ' (at p 11). For some possible technological solutions in order to avoid 'passage' through certain countries see T. Maurer et al, *Technological Sovereignty*, *supra* note 17, at pp. 58 ff.

[26] See O. Pollicino, M. Bassini, *The Law of the Internet between Globalisation and Localisation*, in M. Maduro, K. Tuori and S. Sankari (eds), *Transnational Law: Rethinking European Law and Legal Thinking*, Cambridge University Press, 2014, 346 (advocating, at pp 372f, the principle of mutual recognition). See also O. Lynskey, *The Extraterritorial Impact of Data Protection Law through an EU Law Lens*, in F. Fabbrini, E. Celeste, J. Quinn, *Data Protection Beyond Borders. Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Ch 12.

[27] The issue of 'digital extraterritoriality' is discussed, and challenged, by A. Aguinaldo and P. De Hert, *European Enforcement and US Data Companies*, in F. Fabbrini, E. Celeste, J. Quinn, *Data Protection Beyond Borders. Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Ch 10, who appropriately analyse the applicability

in one of the most ancient and long-lasting international treaties, the 1884 Convention for the Protection of Submarine Telegraph Cables. More important is the status of satellites under international space law, considering that increasingly satellites are used to receive, process and store data which must be easily and quickly retrievable at a global level (the 'cloud' metaphor is indicative)[28].

6. *Fora*

New issues such as FFD require that one should try to think out of the box. Lawyers have an innate path dependency – which explains why Roman law is still so strong – which preserves them and their role in society. Clearly one should not start everything from scratch and re-invent the wheel. However, an evolutionary and adaptive approach appears to be more rewarding than simply putting data into a Procrustean bed and bending it to a pre-digital notion. To do this the fora where appropriate solutions can be forged are very important and all can give a converging contribution.

WTO. It has been pointed out why well-established principles of international trade are difficult to adapt to FFD, and the rather poor results provided by the GATS treaty were highlighted, together with the paralysis of the Doha Round. However, if one looks at FFD in a broader trade perspective one can easily understand that in order to find an agreement there is a natural tendency to find a quid-pro-quo. This was the sense of the draft of the Trans-Atlantic Trade and Investment Partnership (TTIP) between the EU and the USA before it was dumped in 2016 by all the candidates (both Democrat and Republican) for the US presidency. The provisions on cross-border information flows and localisation of infrastructures – which

to digital communications of the 1927 landmark decision of the Permanent Court of International Justice in the Franco-Turkish dispute concerning the steamship *Lotus*. However, seen from the perspective of 'harmful acts' that warrant a military reaction, the conclusion might significantly differ (see W. Heintschel von Heinegg, *Legal Implications of Territorial Sovereignty*, *supra* note 24; and very recently F. Delerue, *Cyber Operations and International Law*, Cambridge University Press, 2020, at pp. 214 ff.)

[28] One could add the billions of billions of data lost in the 'datasphere': see J-S Bergé, S. Grumbach and V. Zeno-Zencovich, *The "Datasphere", Data Flows beyond Control, and the Challenges for Law and Governance*, in *European Journal of Comparative Law & Governance*, vol. 5, 144, 2018; analysed also by O. Ben-Shahar, *Data Pollution*, in *Journal of Legal Analysis*, vol. 11, 104, 2019.

clearly favoured American big-tech companies[29] – were balanced with greater access of EU exports to the US. Trade negotiations highlight common interests and a practical, rather than ideological, terrain of discussion[30].

OECD. The Organization for Economic Cooperation and Development has devoted numerous documents and analysis to the FFD, starting from the 2014 'Principles for Internet Policy-Making'[31]. More recently it has tried to indicate how to bridge the differences in what it classifies as the 'four broad approaches' to the regulation of cross-border data flows[32]. The role of FFD in broader context has been set out in the February 2020 report on 'Going Digital. Integrated Policy Framework'[33], where great attention is devoted to the relationship between personal data protection and interna-

[29] See the joint *European Union-United States Trade Principles for Information and Communication Technology Services* statement of 4 April 2011 at: 2009–2017.state.gov/p/eur/rt/eu/tec/171020.htm.

[30] In favour of the WTO as the forum in which to tackle the issues of cross-border flow of information, see S. A. Aaronson, *What Are We Talking About When We Discuss Digital Protectionism?*, ERIA Paper, 14 July 2017 (available on SSRN at: papers.ssrn.com/sol3/papers.cfm?abstract_id=3032108).

[31] Available on-line at: <http://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf>. The document indicates among its objectives the promotion and protection of the global free flow of information and the cross-border delivery of services.

[32] See the document on *Trade and cross-border data flows* prepared by the Working Party of the Trade Committee (December 2018) (available on-line at: <http://www.oecd.org/offi cialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)19/FINAL&docLanguage=En>). The four approaches are: 'At one extreme, there is the absence of cross-border data flow regulation, usually because there is no data protection legislation at all (largely in least developed countries). While this implies no restrictions on the movement of data, the absence of regulation might affect the willingness of others to send data. The second type of approach does not prohibit the cross-border transfer of data nor does it require any specific conditions to be fulfilled in order to move data across borders, but it provides for ex-post accountability for the data exporter if data sent abroad is misused. A third type of approach conditions the flow of data by permitting transfers only to countries that have received an adequacy determination (i.e. a public or private sector finding that the standards of privacy protection in the receiving country are adequate), and/or in the event that appropriate private sector safeguards, such as contractual mechanisms, are provided, or in the case of some narrow exceptions. The last broad type of approach relates to systems that only allow data to be transferred on a case-by-case basis and subject to a review and somewhat discretionary approval by relevant authorities. This approach relates not only to personal data for privacy reasons but also to a more sweeping category of data referred to as "important data", including in the context of national security'. The report contains numerous very useful tables and charts.

[33] Available at: <http://www.oecd-ilibrary.org/docserver/dc930adc-en.pdf?expires=1584271633&id=id&accname=guest&checksum=06106FF6E578EB42FB6AB8C-166B7EE2B>.

tional data-driven innovation and the role that the OECD guidelines on the 'Transborder Flows of Personal Data' may have[34]. Clearly the role of the OECD in this field, as in many others, is mostly one of expert suasion. However, the circular process of formation of its guidelines and policies (from national experts to the institution, and from there to its Members) should not be underestimated.

G20 Summits. To these one should add – because of its high political level – the G20 Summits. In particular, the 2019 Osaka summit issued a final statement which expressly tackles the FFD issue, under the chapter devoted to 'Innovation: Digitalization, Data Free Flow with Trust':

> Cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development, while raising challenges related to privacy, data protection, intellectual property rights, and security. By continuing to address these challenges, we can further facilitate data free flow and strengthen consumer and business trust. In this respect, it is necessary that legal frameworks, both domestic and international, should be respected. Such data free flow with trust will harness the opportunities of the digital economy. We will cooperate to encourage the interoperability of different frameworks, and we affirm the role of data for development. We also reaffirm the importance of interface between trade and digital economy, and note the ongoing discussion under the Joint Statement Initiative on electronic commerce, and reaffirm the importance of the Work Programme on electronic commerce at the WTO[35].

ITU. Because of its high technical expertise and its constant interaction with the WTO, the International Telecommunications Union (ITU) is another forum which appears to be indispensable in order to set out rules in the field of FFD. One has repeatedly noted that although the provision of telecommunication services and the collection and processing of data are strongly inter-related, they follow different logics and models: the former

[34] See the *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 2013 (available at: http://www.legalinstruments.oecd.org/public/doc/114/114.en.pdf>).

[35] For a first comment, with interesting charts and economic data, see T. Fukunaga, *DataFree flow with Trust and Data Governance* (available at: <http://pecc.org/resources/digital-economy/2616-datafree-flow-with-trust-and-data-governance/file>); and J. Sugawara, *Launch of 'Osaka Track' on Digital Rules. Many difficulties lie ahead for WTO e-commerce negotiations*, a Mizuho Research Institute paper (2 July 2019) (available on-line at: <http://www.mizuho-ri.co.jp/publication/research/pdf/eo/MEA190726.pdf>).

are the object of the activity; the latter are its result. They are kept together by the technology and by the standards which ITU helps set at an international level. The involvement of ITU is also important because private parties are important stakeholders in its legal process.

7. *Conclusion*

In conclusion, free-flow of data presents too many novel aspects and a mixture of competing interests (individual rights, international trade, national and security exigencies)[36] all of which suggest that it would be preferable reasoning from a clean slate on which one should write appropriate rules extracted from existing models rather than bending and distorting the highly successful international trade laws for purposes and situations which are quite dissimilar in form and in substance.

[36] Similar concerns are expressed by M. Burri, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, *supra* note 8, who points out (at p 130) that the traditional 'analog regulatory venues' are at odds 'with the unpredictable, scruffy, dynamic, and open innovation of digital platforms and data that flows regardless of state borders'. 'Beyond the province of the economy and even in seemingly technical decision-making – such as for classification or localization requirements for foreign operators – essential rights and values like freedom of expression, privacy, fairness, equality of opportunity, and justice, will be affected'.

Vincenzo Zeno-Zencovich

Data protection[ism]

1. *Introduction: The Problem*

Protectionism is a policy which aims at protecting domestic industries limiting – or excluding – importation of goods or provision of services from third countries. It can sometimes manifest itself by limiting exports of certain materials or products which, included in a different product, may enable third countries to compete more effectively in the exporting country or on the world market.

Given this very broad and commonly shared definition, can one speak of a current "data protectionism?"[1]. An analysis of this topic appears to be important to understand the real nature of data and their relevance not only in international trade relations but also in global geopolitics.

If one looks at the most common and historical form of protectionism, i.e. high import tariffs or quotas on the importation of foreign goods, one immediately understands that this cannot apply to data, for a multitude of reasons:

a) In the first place, data are non-material and therefore do not encounter any sort of customs control[2]. The mere idea of "counting" the data (by digital units, i.e. bytes) make very little sense, because their value does not depend on their size, but on the information they convey or are used for (data on the distribution and sales of groceries in Sweden are of practically no use in South Africa).

b) To be even more precise, the value of data is near to zero without programmes that are able to analyze them and extract the information – past, present or future – which is needed. Clearly one

---

* This article was first published in *MediaLaws. Rivista di diritto dei media*, 2, 2022, pp. 1-8.

[1] See S.A. Aaronson, *What Are We Talking about When We Talk about Digital Protectionism?*, in *World Trade Review*, 18, 2019, 541.

[2] «Trade in data is different from trade in goods and other services. Data are intangible, highly tradeable, and some types of data, when processed, are a public good, which governments must provide and regulate effectively» (S. A. Aaronson, *What Are We Talking about When We Talk about Digital Protectionism?*, ivi, 543.

could, hypothetically, prevent the use of foreign data analytics in one's territory, but – setting aside the difficulties in implementing such a measure – what would be its economic sense? Would it protect the domestic digital industry?

c) But even imagining that data (whether bulk or selected) was sold as a commodity which is scarce in the domestic market (Country A does not have enough data which it needs, and therefore imports it from country B), the protectionist measure would be aimed not at protecting the domestic data industry, but at avoiding that data be collected in country A and processed in country B to be used for economic activities in country A or elsewhere. The point is that no country objects to the importation of data concerning other countries and their processing and extraction of value on its own territory. The concern – as we shall see – is not about data imports, but about data exports[3].

If one looks at the legal framework in which international trade of data could be placed, it appears very clear that the three pillars of the GATT treaty (Article I: Most Favoured Nation principle; Article III: National Treatment principle; Article XI: Elimination of quantitative restrictions) are hardly applicable to data. Not only for their non-material nature, but also because one can easily understand the difficulties of qualifying data as a like product as the difference is not in their content, but in the software that can analyze them and extract the relevant information. The same can be said for a hypothetical, but unrealistic, discrimination between imported data and domestic data «so as to afford protection to the domestic production».

As to quantitative restrictions on imports – whatever their protectionist function might be – as one has said such kind of measurements appear to be without any economic sense.

One is therefore driven out of the barren field of international trade in goods, and directed to that of international trade in services. But neither such different perspective appears to be more fruitful.

Let us assume that the service consists in the collection, storage, processing and output of data and in all the connected downstream services (e.g. quality control, maintenance and assistance, metering, marketing etc.).

The protectionist measure would be that of excluding third country

[3] M. Burri, *Data Flows and Global Trade Law*, in Ead. (ed.), *Big Data and Global Trade Law*, Cambridge, 2021, at 12: «The new generation of Internet controls seeks to keep information from going *out* of a country, rather than stopping it from entering the sovereign state space» [italics in the original].

businesses from providing such services, or limiting the number of third country providers, or the quantity (whether in terms of operations or of value) of services provided.

These services need to be carefully distinguished in their relationship with data.

1. In some cases, such services are essential – but ancillary – for the provision of a different service. The best example is that of financial services where the transaction cannot be completed without collecting storing, and processing the data of the parties involved.
2. In other cases, such services are ancillary to the correct functioning of a material product. The whole IoT world moves around the integration between a physical object and the data it collects, receives, processes and make it operate correctly. The best example is a Tesla automobile which is, substantially, a data management software applied to a bodywork and to a mechanical machinery.
3. There are then to be considered services which nearly entirely consist in the provision of certain ICT services on the basis of/in exchange for the data which is provided by the user[4].

The first case falls under the extensive legislation, both domestic and international, on the provision of such paramount services. If a country decides – and the list of such exemptions is endless – to restrict the provision of certain services – typically financial ones – the reasons are related to its financial policies (balance of payments, currency stability, protection of the domestic banking system), not to some form of data protectionism.

The second case can be divided in two further sub-cases. That in which the protectionist measure (high tariffs, quotas) is introduced to protect domestic industry of a like product (e.g. refrigerators, industrial robots) which uses – like practically all nowadays – IoT technologies. In this sub-case data are not at the center of the trade issue.

In the other sub-case, the protectionist measure is taken not because one wants to protect the domestic industry in the like product, but because one wishes to control the use of the data. The limitation therefore has to do with compliance with domestic data legislation and especially with provisions concerning the transfer of data to third countries. Hypothetically such transfer could be completely independent from the provision of the

[4] See also the classification proposed by S. Aaronson, *What Are We Talking about When We Talk about Digital Protectionism?*, cit., 568, who lists five types of data: Personal data, Confidential business data, Public data, Metadata, Machine-to-machine communication.

service (which is ensured by digital technologies operating in the country of importation), but is considered, very simply, an informational asset of the business, to which it is entitled.

A similar situation presents itself in the third case, where data collection, storage, and processing are the core of the business of the services of the business, which commonly is designed as a data company.

Although it is quite common to identify such companies in the two internet giants such as Facebook and Google, one should point out that there are hundreds, if not thousands, of other companies who operate on a similar business model: they provide a service on the basis of/in exchange of data. It is sufficient to take a look at the dozens of applications every user downloads on his or her computer (Adobe, anti-virus, etc) or smartphone (maps, weather, entertainment, etc.) to realize the vastity of the phenomenon.

Again, the protectionist measure is aimed at ensuring compliance with domestic regulations on data processing and limiting the transfer abroad of data.

If one places all these cases within the context of the GATS Treaty (and not considering its very poor performance over the last 25 years, which borders irrelevance) one realizes that its provisions do not seem to apply to services which include, to a varying extent, data collection, storage and processing[5].

At any rate, one could find various provisions in the GATS Treaty which appear to justify restrictive policies. In the first place, the principle of non-discrimination is not violated if the restrictions to the transfer or data apply to any business, whether domestic or foreign (Articles VI and XVIII). In the second place, Article III bis (Disclosure of Confidential Information) and Article XIV (General Exceptions) appear to justify such measures. In particular, the latter provision expressly states that «nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures (…) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: (…)

> (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.

To sum up what has been so far presented, it would seem that both the GATT and the GATS Treaties, with their countless annexes, do not appear

[5] «GATS is not sufficiently adaptable to a data-driven economy» (A.D. Mitchell - N. Mishra, *WTO Law and Cross-Border Data Flows: An Unfinished Agenda*, in M. Burri (ed.), *Big Data and Global Trade Law*, cit., p. 93).

to be relevant in the case of what has been, ex hypothesis, described as data protectionism.

The reasons of such meagre result do not depend on a defective or obsolete drafting of the two texts, but on the very nature of data and their role in global economy and geopolitics.

On the one hand one has pointed out that data, as a non-material entity appear difficult to regulate. Their sheer quantity – which by rule-of-thumb is calculated in zettabytes –, their constant, *ad infinitum*, production, their ubiquity, the ease in reproduction and transfer render data an unicum in the history of mankind. For this reason, the definition of datasphere – in which data circulate with little or no control – appears to be appropriate[6]. Surely data economics are an essential part of today's economy, but precisely for this reason they need to find an appropriate classification.

Just as in any business – since the most ancient times – information (extracted from the available data) is an essential element and is variously protected (confidentiality agreements, trade-secrets, know-how), in any country the data concerning whatever happens in it concerning its territory, its entities, its citizens have a strategic importance. Just as States claim sovereignty over their land, their skies, their territorial waters, they extend such sovereignty to the non-material world of data.

The reasons for this expansion are far from trivial.

In the first place there are security concerns. Data provide sensitive information concerning the localization, nature and efficiency of security facilities. But even more, they reveal qualities and fragilities of the data transmission infrastructures, which, *per se*, are critical in any national security assessment. Cybersecurity becomes therefore a foremost goal to be advanced through the control of the data processing servers[7].

But even if one looks at the data produced in/by a country from a purely economic perspective, knowledge of such data, in a predictive analytics context, reveals the general situation, societal and economic trends, imminent crisis, foreseeable strategies.

Those who hold such data have an informational advantage which can be easily exploited. One could divide countries between "data empires" and "data colonies", and very few are happy to fall in the latter category[8].

[6] See J-S. Bergé - S. Grumbach - V. Zeno-Zencovich, *The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance*, in EJCL&Gov., 5, 2018, p. 144.

[7] See P. Swire - D. Kennedy-Mayo, *The Effects of Data Localization on Cybersecurity*, in ssrn.com, 2022.

[8] «Digital colonialism is traditional colonialism revisited» (A. Bhatt, *Data Sovereignty: The Quintessential Model for the New World Order*, in *Indian Law Institute Law Review*, 6,

This is the ultimate reason for "data protectionism". The aim is that of protecting not a domestic industry but national sovereignty[9]. A country that allows free access to its data resources could be compared to a country that allows the exploitation of its natural resources only to buy them back once they have been processed.

Once one has outlined the rationale of data protectionism and withholding any value judgment on its desirability or effectiveness, it is important to lay out the ways through which this policy is implemented.

The first is that is commonly called "data localization"[10]. The term indicates that data collected in a certain country may be stored and processed only in that country. This means that the data may not be transferred abroad.

In this case there is no limitation to who is providing this service – and therefore there is no discrimination in access to the market of data processing services[11] – but "simply" the obligation not to transfer such data abroad.

Data localization is labelled as being against free trade, and one finds several international instruments which explicitly prohibit such practice. But if one looks at the rule in a pragmatic way, free flow of data is not really about trade[12].

Data is not sold, nor bought. Data is simply a resource on which to develop economic and marketing strategies.

The service *per se*, consisting in collecting, storing and processing data, is in no way prevented. The parallel could be that – very common in the past

2021, 285, at p. 287. And see now S. Grumbach, *L'empire des algorithmes*, Paris, 2022).

[9] According to H. Gao, *Data Sovereignty and Trade Agreements: Three Digital Kingdoms*, in ssrn.com, 2021, the three great economic regions (US, RPC and EU) champion, respectively, the sovereignty of the firm, of the state and of the individual. This paper argues that, at the end of the day, all three models strive to ensure sovereignty of the state.

[10] For a wide survey and analysis of the various data localisation measures and their rationale see H. Ursic - R. Nurullaev - M. Olmedo Cuevas - P. Szulewski, *Data localisation measures and their impacts on data science*, in V. Mak - E. Tjong Tjin Tai - A. Berlee (eds.), *Research Handbook in Data Science and the Law*, Cheltenham – Northampton (MA), 2019, p. 322.

[11] But consider that certain researches indicate that «the establishment of local data centres does not appear to lead to new jobs created in the country» (M.F. Ferracane, *The Costs of Data Protectionism*, in M. Burri (ed.), *Big Data and Global Trade Law*, cit., p. 70).

[12] See, however, the economic analysis by S. R. Potluri - V. Sridhar - S. Rao, *Effects of Data Localization on Digital Trade: An Agent-Based Modeling Approach*, in *Telecommunications Policy*, 44(9), 2020, according to whom «there is often clustering of consumers around local firms in highly restrictive data localisation regimes, thus enabling local firms to effectively compete against global multinationals. However, results also indicate that while free cross-border data enables intense competition amongst producers, data localisation restrictions often limit consumer choice due to its effect on price and quality of services».

– of prohibiting the export of profits made by a foreign company operating in a third country. This practice is expressly prohibited by Article VIII of the IMF Treaty, but this points out that an international agreement is required to impose free flow of data[13]. If it is lacking, it is doubtful whether one can claim some violation of the very vast and consolidated international trade system[14]. In a few words: data localization is aimed at protecting national interests and, provided it is not discriminatory, it does not appear to violate international trade law[15].

An indirect way of imposing data localization is that adopted by the European Union with its pervasive personal data regulation.

One should point out that the notion of "personal data" is established by the EU and member States institutions (CJEU, EDP Supervisor, EDP Board, National Data Protection Authorities) and is expansive, encompassing more and more data. The truth is that practically all data is "personal data" in the sense that it leads to identifiable natural persons[16]. The only data that would appear to fall outside the definition of the "data subject" given by Article 4, para. 1, of the GDPR, are those concerning the weather or other natural phenomena and aggregated statistical data. And the fact that the GDPR expressly limits its scope to natural persons, does not liberalize processing of data by legal entities in B2B relations, because the businesses would have to previously delete all the data concerning the natural persons involved in the transaction (the legal representative of another entity, the contact person, etc.). A very costly operation, which – coupled with the draconian sanctions imposed with the greatest of ease by the various authorities – is, in substance, discouraged.

[13] See the lengthy paragraph devoted by M. Burri, *Data Flows and Global Trade Law*, cit., 24 ss., to data-related rules in Preferential Trade Agreements (PTAs); and M. Elsig - S. Klotz, *Data Flow-Related Provisions in Preferential Trade Agreements*, in M. Burri (ed.), *Big Data and Global Trade Law*, cit., p. 42.

[14] I have tried to present the argument in more detail in V. Zeno-Zencovich, *Free-Flow of Data. Is International Trade Law the Appropriate Answer?*, in F. Fabbrini - E. Celeste - J. Quinn (eds.), *Data Protection Beyond Borders*, Oxford, 2021, p. 173.

[15] M.F. Ferracane, *The Costs of Data Protectionism*, in M. Burri (ed.), *Big Data and Global Trade Law*, cit., 76, presents a similar arguments more elegantly: «The debate on whether data restrictions represent a trade barrier that could potentially be challenged at the WTO is, however, still in its infancy».

[16] Quite appropriately M. Burri, *Data Flows and Global Trade Law*, cit., reminds us (at 14) that «in reality it is now rare for data generated by user activity to be completely and irreversibly anonymized« and that «big data enables the reidentification of data subjects by using and combining datasets of nonpersonal data, especially as data is persistent and can be retained indefinitely with the presently available technologies».

Once one has established that practically all data are "personal data", the further step is that of prohibiting transfer of data to third countries which do not ensure «an adequate level of protection» (article 45 GDPR). And when one looks at the criteria used in article 45, para 2, to assess the «adequacy of the level of protection» it is difficult to find more than half a dozen countries, among the remaining 166 members of the UN, that pass muster. The best evidence is the inglorious fate of the "Safe Harbour" and of the "Privacy Shield" agreements of the EU with its most important political and economic partner, the US, both struck down by the EU Court of Justice[17]. A similar effect had already been achieved by the CJEU famous Google Spain[18] decision when it stated that the mere collection of commercial ads in a Member State was tantamount to be established in the EU, and therefore Google was considered subject to EU data protection laws.

The result is, de facto, a data localization principle, which is reaffirmed in the hoard of new "Digital Acts" proposals, to which one should add the very strong political pressure for the creation of an "European Cloud", which in its mere denomination implies a localization principle[19].

Setting aside comments on the rather hypocritical preach good and scratch bad approach to free flow data, one easily understands that under the cloak of fundamental rights (personal data protection enshrined in Article 8 of the EUCFR) there is the quite understandable need to avoid that the EU become even more a colony of ICT super-powers, the US and the RPC.

In the dualism empire/colony one can read the coherent and constant US policy against data localization which one finds in most of the international trade treaties it has promoted over the last 20 years and in innumerous policy statements[20]. The reasons are quite obvious: The US

[17] See G. Resta, - V. Zeno-Zencovich (eds.), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"* , Rome, 2016.

[18] See G. Resta - V. Zeno-Zencovich (eds.), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Rome, 2015.

[19] See the 15 October 2020 Declaration by the 27 Member States on "Building the next generation cloud for businesses and the public sector in the EU": «Cloud computing provides the data processing capacities required to enable data-driven innovation, hence the urgent need to cooperate to foster Europe's technological sovereignty and to ensure that our businesses and public sector have access to resilient and competitive data storage and processing capacities. Europe's leadership in this area is essential to enable artificial intelligence, Internet of Things and 5G/6G. Europe should aim to set global norms on data storage and processing and to maintain market openness and international cooperation».

[20] See, *ex multis*, Chapter 19 of the 2019 US-Mexico-Canada Trade Agreement (USMCA),

are the leaders in data processing and the "Big Data revolution" started in the US. Its digital industry is a world leader and has all the interest in broadening its market, both for collecting data and for selling the results of its analytics[21]. For the moment being they do not appear to fear that their data be collected and processed in third countries. Their main technological competitor being the RPC the action taken has been that of challenging "back-door" access to data through Chinese technology (e.g. Huawei). This substantially introduces a localization principle, preventing transfer of data to certain countries. As to Europe the US response to the territoriality principle of the GDPR has been the so-called CLOUD Act[22] which enables US authorities to access data held by any US company or affiliate wherever in the world.

The tit-for-tat approach in data control is manifest in the EU response to the US worldwide access. The "free flow" of non-personal data Regulation applies to any provider even if not established in the EU[23]. The Digital Services Act proposal (DSA) imposes on providers of intermediary services that are established in a third country and offer services in the EU to designate a legal representative in the Union and provide all the information on their legal representatives[24]. The proposed Artificial

according to which «No Party shall require a covered person to use or locate computing facilities in that Party 's territory as a condition for conducting business in that territory». One finds similar provisions in the most recent trade agreements signed by the US.

[21] See S.A. Aaronson, *What Are We Talking about When We Talk about Digital Protectionism?*, cit., p. 549.

[22] HR 4943 – Clarifying Lawful Overseas Use of Data Act (CLOUD Act) (available at the US Congress website congress.gov). According to § 2713 «A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States».

[23] Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union, Article 2: «This Regulation applies to the processing of electronic data other than personal data in the Union, which is: (a) provided as a service to users residing or having an establishment in the Union, regardless of whether the service provider is established or not in the Union».

[24] Regulation on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, Article 11: «Providers of intermediary services which do not have an establishment in the Union but which offer services in the Union shall designate, in writing, a legal or natural person as their legal representative in one of the Member States where the provider offers its services».

Intelligence Act explicitly extends its rules to providers and users of AI Systems that are established in a third country if their results are used in the EU[25].

The Data Governance Act proposal states that judgments of courts or administrative authorities of third countries requiring access to non-personal data should be enforceable only if there is an international agreement in that sense[26].

The Data Act proposal repeats such principle adding, significantly, that the provision is imposed to protect not only fundamental rights of EU citizens but also national security, intellectual property rights, trade secrets, commercial confidentiality[27].

* * * *

The analysis conducted in the previous pages brings to conclude that "data protectionism" has much more to do with international politics than with international trade. In this sense it can be associated with the never-ending saga of Foreign Direct Investments, at times invoked as a blessing, in others seen as a curse, and which sways between very substantial incentives and rigorous vetoes. In the latter case what is at stake is the industrial or financial sovereignty of a country. With data – owing to their polyfunctionality and non-materiality – the concern covers the entire spectrum of public and private activities.

This does not imply downplaying the economic relevance of free flow of

[25] Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Article 2: «This Regulation applies to:
(a) providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country;
(b) users of AI systems located within the Union;
(c) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union».

[26] Regulation on European data governance (Data Governance Act), Article 30: «Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a public sector body, a natural or legal person to which the right to re-use data was granted under Chapter 2, a data sharing provider or entity entered in the register of recognised data altruism organisations to transfer from or give access to non-personal data subject to this Regulation in the Union may only be recognised or enforceable in any manner if based on an international agreement».

[27] Regulation on harmonised rules on fair access to and use of data (Data Act), Article 27, para. 3: A EU competent authority will decide «when it considers that the decision may relate to commercially sensitive data, or may impinge on national security or defence interests of the Union or its Member States».

data, but points out that the solution can be found only in new and shared principles enshrined in international law agreements[28]. Which, for the very troubled times we are all experiencing, appears to be wishful thinking[29].

[28] S. A. Aaronson, *Data Is Different, Policymakers Should Pay Attention to Its Governance*, in M. Burri (ed.), *Big Data and Global Trade Law*, cit., 359: «The world is awash with data and there is no consensus on how to regulate it».

[29] M. Burri, *Data Flows and Global Trade Law*, cit., 14: «The striking divergences both in the perceptions and the regulation of privacy protection across nations and in particular between the fundamental rights approach of the EU and the more market-based, non-interventionist approach of the United States have also meant that conventional forms of international cooperation and an agreement on shared standards of data protection have become highly unlikely». And her conclusive words: «Data issues cannot be covered by the mere 'lower tariffs, more commitments' stance in trade negotiations but entail the need for reconciling different interests and the need for oversight. In this context, while the paths for engaging in and advancing regulatory cooperation would ideally be followed in the multilateral forum, preferential trade venues can serve as governance laboratories. The way forward may be truly bright but remains highly (and perhaps unfortunately so) dependent on the role that the key players, the United States, the EU and China, are willing to assume» (at 41).

SECTION IV
Data Governance

Davide Zecca, Licia Cianci

Right to information, online speech and democratic political processes: a legal framework for Europe and beyond?

Abstract: The fairness of political processes, which in modern deliberative democracies depends on the existence of pluralism in the political discourse, is threatened in the digital environment by micro-targeting techniques and disinformation campaigns, which alter the authenticity of the public debate and influence the political orientation of the public opinion. Discussing the role of digital intermediaries in this context is therefore crucial for European countries and institutions in order to ensure the long-term survival of pluralistic democracies. Patterns of State regulation of freedom of expression online are therefore weighed against trends of platforms' self-regulation to assess whether the EU is laying down an effective strategy to neutralize phenomena otherwise undermining democratic processes.

1. *Introduction*

A defining feature of modern forms of State in the Western legal culture is the enfranchisement of citizens increasingly taking part to the determination of public policies, albeit only indirectly through the system of representative democracy[1]. This mechanism has worked effectively because, on one side, free debate and exchange of ideas have been allowed

---

[*] A revised version of this article was first published as *Polluting the political discourse: what remedies to political microtargeting and disinformation in the European constitutional framework*, 10 *European Journal of Comparative Law and Governance* 1 (2023).
While the considerations developed in the article are common to the authors, Licia Cianci authored §§ 2, 3, 4; Davide Zecca authored §§ 5, 6, 7. The Authors have written jointly § 1. The Authors have benefitted from the support of the Project PRIN 2017: GOVERNANCE OF/THROUGH BIG DATA: CHALLENGES FOR EUROPEAN LAW. A revised version of this article will be published in 10 European Journal of Comparative Law and Governance 1 (2023) with the title "Polluting the political discourse: what remedies to political microtargeting and disinformation in the European constitutional framework?"

[1] For a synthetic accounts of different varieties of constitutional democracies, see G. Frankenberg, *Democracy*, in M. Rosenfeld-A. Sajó (eds.), *The Oxford Handbook of Comparative Constitutional Law*, Oxford, Oxford University Press, 2012, 250-268.

and encouraged while, on the other, the flourishing of traditional mass-media has created an environment where several viewpoints may be put forth and the public opinion is shaped through discussion of the topics that are deemed most relevant by a majority of the population[2]. In short, the existence of freedom of speech and freedom of the press, together with freedom of (political) association, is the backbone of the democratic pluralistic form of State.

Against such a backdrop, due consideration must be given to the evolution of the ways of communication that, over the last decades, has shaken the foundations of this model. More specifically, this paradigm is questioned in light of an array of phenomena that endanger the authenticity of public debate, thereby undermining the full functioning of the dynamics shaping the public opinion. The true revolution lies in the transition from the so-called Web 1.0 – based on a unidirectional model of information, where users are mere recipients of news filtered by media outlets – to the so-called Web 2.0 – whose distinguishing feature is the existence of user-generated content[3]. This trend is evident just by looking at the extraordinary number of subscriptions to social networking platforms, which make the latter simultaneously among the most visited websites all over the world, while also encompassing more users than the population of most countries on Earth[4].

The concern is that discussion, debate and the formation of political beliefs occur overwhelmingly on these platforms which, while all providing for more or less detailed terms of conduct, potentially allow for unregulated speech. If, on the one hand, this might be considered beneficial for the

[2] The necessary correlation between democracy and pluralism has been underlined, among many others, by the European Court of Human Rights in *Refah Partisi (the Welfare Party) and Others v. Turkey* [GC] – App no 41340/98, 41342/98, 41343/98 et al., Judgment of 13 February 2003, § 89. The Court of Strasbourg had already illustrated the broad perimeter of freedom of expression under the Convention in *Handyside v. United Kingdom* [GC] – App. no 5493/72, Judgment of 7 December 1976.

[3] C.E. George, J. Scerri, *Web 2.0 and User-Generated Content: legal challenges in the new frontier*, *Journal of Information, Law and Technology* 2 (2007); A. Darwish, K.I. Lakhtaria, *The Impact of the New Web 2.0 Technologies in Communication, Development, and Revolutions of Societies*, in *Journal of Advances in Information Technology*, vol. 2, 204-216, 2011, doi:10.4304/jait.2.4.204-216.

[4] As of January 2022, Facebook has over 2.9 billion users registered, while also YouTube, WhatsApp, Instagram, WeChat and TikTok exceed 1 billion monthly users, whereas only two countries (China and India) exceed this threshold, see Global Social Media Stats (https://datareportal.com/social-media-users) and Countries in the world by population (2022) (https://www.worldometers.info/world-population/population-by-country/).

purpose of the preservation of a lively and caring public opinion, on the other hand, such easy access to a tool able to disseminate speech to the whole world presents crucial challenges that need to be faced timely by Western societies to ensure the survival of pluralist democracies[5].

Among the risks mentioned, there is the increasing resort by political actors to micro-targeted advertisements, *i.e.*, political messages aimed at garnering voters' support and tailored to meet the users' policy preferences. This kind of electoral communication is made possible by the structure of social networking platforms, which can build very accurate profiles of the users and are able to show them content that enhances the already existing beliefs. The more data is available to the algorithm, the more users are in danger of ending up locked into 'echo chambers'. The fairness of the public debate may also be poisoned by the circulation of misleading or inaccurate information that is usually sensationalist and unverified. The viral spreading of 'fake news', often framed in order to stir visceral reactions and therefore lacking careful fact-checking, is capable of influencing the outcome of elections or public policy choices[6].

The present article is not built on the misunderstood assumption that the scope of application of free speech rights, envisaged in Western countries, exhausts the models of political communication and the dynamics of electoral processes in the comparative panorama. The existence of legal systems that severely curtail the access to digital media or that ensure that only State-operated social networking platforms are accessible is fully acknowledged (*e.g.*, the so-called Great Firewall of China[7]). Also, attempts to establish a digital autarchy that sets a country free from the infrastructure upon which Internet is based are currently being undertaken (*e.g.*, Russia's attempt to build an alternative system of information technology communication[8]). Yet, the awareness about these alternative

[5] A. Koltay, *The Protection of Freedom of Expression from Social Media Platforms*, in *Mercer Law Review*, vol. 73, 2, 2022, Article 6, available at: https://digitalcommons.law.mercer.edu/jour_mlr/vol73/iss2/6.

[6] H. Margetts, *Rethinking Democracy with Social Media*, in *The Political Quarterly*, vol. 90, 107-123, 2019, https://doi.org/10.1111/1467-923X.12574.

[7] R. Creemers, *The Privilege of Speech and New Media: Conceptualizing China's Communications Law in the Internet Era*, in J. DeLisle, A. Goldstein, G. Yang (eds.), *The Internet, Social Media and a Changing China*, Philadephia, University of Pennsylvania Press, 2016, available at SSRN: https://ssrn.com/abstract=2379959 or http://dx.doi.org/10.2139/ssrn.2379959.

[8] L. Sivetc, *State regulation of online speech in Russia: the role of internet infrastructure owners*, in *International Journal of Law and Information Technology*, vol. 27, 1, 28–49, 2019, https://doi.org/10.1093/ijlit/eay016.

paths to conceive political processes and the establishment of intrusive mechanisms of State censorship on free speech, especially in politically sensitive matters, does not imply that these different constitutional sensitivities shall be taken into account in the assessment of the most suitable regulatory models of free speech online, at least in Europe. On the contrary, it is exactly the different understanding of the role of freedom of speech in the dynamics of popular participation in public policymaking that advices against comparing these authoritarian models with Western deliberative democracies built on informational pluralism[9].

In light of all the above, the present article will set off from an assessment of the theories justifying a broad recognition of free speech (§2), together with an accurate reconstruction of the scope and the interpretation of constitutional provisions protecting freedom of speech and information in the European Union (EU), European Convention on Human Rights (ECHR) and US legal frameworks (§3). Then, the technical mechanisms underlying the functioning of political micro-targeting will be analysed, taking into account existing regulations or applicable standards of review at supranational and domestic level in Europe (§4). The extent to which disinformation campaigns are capable of affecting the electoral preferences of voters will be discussed, also by giving account of the actual legislation passed to mitigate the spread of the phenomenon in Europe (§5). An illustration of the past and prospective EU approach to freedom of information in the online environment will then be provided (§6). Eventually, a set of possible models to regulate free speech online so that a pluralist informational environment remains in place is analysed, supplemented by considerations on the role of State legislation and self-regulation of private actors to ensure the fairness of online public discussion for political processes that are actually democratic (§7).

2. *Theoretical foundations and comparative constitutional perspectives of freedom of speech: the European and the US framework*

Freedom of expression[10] and the right to receive information are the

[9] A. Mughan, R. Gunther, *The Media in Democratic and Nondemocratic Regimes: A Multilevel Perspective*, in R. Gunther-A. Mughan (eds.), *Democracy and the Media: A Comparative Perspective*, Cambridge University Press, Cambridge, 2000, 1-27.

[10] In this paper, the syntagms 'freedom of expression' and 'free speech' will be used interchangeably. Yet, it is important to note that the first is used in the European panorama

cornerstones on which democratic societies are rooted. In the attempt to search for the theoretical foundations of free speech, different theories, mainly elaborated within the Anglo-Saxon legal tradition, have been developed[11].

According to some theories, freedom of speech is essential to the discovery of truth. Already in the seventeenth century, John Milton argues against the licensing requirement on books, stating that 'all opinions, yea errors, known, read, and collated, are of main service and assistance toward the speedy attainment of what is truest'[12]. John Stuart Mill's theories understand freedom of speech as a necessary precondition to guarantee truth as a paramount value. The liberal English philosopher argues that any restriction of free speech has to be discouraged, as the truth could rest in the restricted opinion[13].

Only the lively competition of different ideas will eventually bring the best ones to predominate over falsehoods. This perspective is echoed in Justice Holmes' famous dissenting opinion[14], which has had great impact in the development of freedom of speech in the US framework. In this view, freedom of speech primarily relies on the flow of opinions circulating in the free marketplace of ideas, as the best figurative arena for the emergence of truth through the exchange of different opinions.

Critics of this theory have highlighted that it is implausible to confer an absolute value to truth and to argue that the latter always prevails over falsehood.

Another set of theories identifies in the right to freedom of expression the essential mean to assure individual self-fulfillment and to express his or her personality. According to this theory, individuals, as rational and equal human beings, can make autonomous choices[15]. In this sense, it is illegitimate for State powers to interfere and regulate people's autonomous perspectives for the sole reason that their opinions are ignoble or wrong[16].

---

and the latter in the US one.

[11] See E. Barendt, *Freedom of Speech*, 2nd edn, Oxford University Press, Oxford, 2005, 6-23; T. Emerson, *Toward a General Theory of the First Amendment*, in *Yale Law Journal*,vol. 72, 877-956, 1962-1963, 884.

[12] J. Milton, *Areopagitica* in *Areopagitica and other Prose* Works, J.M. Dent, London, 1927.

[13] J.S. Mill, *On Liberty and Other Essays*, Oxford University Press, Oxford, 1991.

[14] *Abrams v. US*, 250 U.S. 616, 630-1 (1919).

[15] K. Greenawalt, *Free Speech Justifications*, in *Columbia Law Review* 1, vol. 89, 119-155, 1989, 150.

[16] R. Dworkin, *Is there a right to pornography?*, in *Oxford Journal of Legal Studies*, vol. 1, 177-212, 1981, 194.

There should be a space, indeed, in which people enjoy the fullest sovereignty over their decisions[17].

A different theory finds theoretical justifications for the right to free speech in the possibility to ensure citizens' participation in the democratic discourse and public decision-making[18]. In this view, access to as much information as possible is crucial for the electorate to form individual and collective judgments over political and social matters, and to subsequently make informed political decisions.

In this perspective, free speech would be essential to ensure concrete and effective possibilities of political participation, while censorship would violate this right to participate in democratic political processes.

Critics of this theory argue that the latter is constructed to protect only political speech, leaving outside other forms of expression[19].

From the analysis of the theoretical foundations of freedom of speech, it emerges how the latter has been traditionally assessed through the lens of the traditional constitutional dialectic between freedom and authority. On one hand, the contours of freedom of speech shall be addressed. On the other, the range of action within which State powers can legitimately restrict free speech shall clearly be defined. The necessity to draw lines between the spaces granted to citizens and to the State is also recreated in the online dimension. Yet, this paradigm of protection is challenged in light of the position of private actors, whose quasi-public role may challenge this traditional dichotomy.

The ideal pluralist environment may be spoilt by the influence of single players in the informational market, which may concentrate an excessive opinion power capable of directing the stances of public opinion on a wide variety of policy matters[20]. Admittedly, the need to prevent excessive concentration of opinion power in the hands of a handful of players

[17] T. Scanlon, *A Theory of Freedom of Speech*, 1 *Philosophy and Public Affairs* 2, 204-226, 1972, 215-222.

[18] A. Meiklejohn, *The First Amendment is an Absolute*, in *Supreme Court Review* 245-266, 1961, 256-257.

[19] J.M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, in *NYU Law Review*, vol. 71, 1–55, 2004, 1.

[20] The issue of opinion power was famously discussed by the German *BundesVerfassungsGericht* in the so-called *Fourth Broadcasting Case* or *Niedersachsen-Urteil* (BVerfGE 73, 118, 4 November 1986), where the Karlsruhe judges held that lawmakers have a constitutional obligation to take measures that prevent the emergence of a predominant opinion power (*vorherrschende Meinungsmacht*), thereby highlighting the dual nature of freedom of expression (negative but also positive freedom, entailing active conducts by State organs).

arose in times where traditional media were still the mainstream source of information. Yet, the emergence of digital intermediaries deserves in-depth analysis under this very same perspective[21].

Under a constitutional standpoint, a relevant concern is whether – and to what extent – political communication and public debate taking place onto social networking platforms affect the right to information in its passive nuance (*i.e.*, the right to be informed). This consideration matters in order to determine whether regulation by public powers is needed to preserve the authenticity of discussions shaping the public opinion and to prevent the poisoning of genuine political discourse by the spread of false information, the manipulation of the news market for partisan purposes and the targeting of specific voters with tailored electoral messages.

Being able to qualify the role exercised by private enterprises that currently own the infrastructures where public discussion mostly takes place is therefore crucial to address the otherwise complicated conundrum that underlies the relationship between private ownership of these platforms on one side and their social and public functions on the other[22]. More specifically, the turning point lies into the identification of the perimeter of State normative reach, thereby drawing a line between the regulatory duties of public powers and the conducts expected (or required by law) by private actors operating digital platforms. If functions that have a traditional public nature, such as that of censorship, are outsourced to private entities, the latter must necessarily be held accountable for the patrolling role that they exercise through the enforcement of content moderation policies[23]. This, in turn, makes it compelling to investigate whether these actors should be required to comply with the high standards of protection of freedom of speech that apply to State institutions under the constitutional framework of each domestic legal system and that of supranational entities (*e.g.* EU, ECHR)[24]. While constitutional provisions usually apply along the vertical axis that connects public powers and private individuals[25],

[21] N. Helberger, *The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power*, in *Digital Journalism*, vol. 8, 842-854, 2020.

[22] G. De Gregorio, *The rise of digital constitutionalism in the European Union*, in *International Journal of Constitutional Law* 1, vol. 19, 41–70, 2021.

[23] M.K. Land, *Against Privatized Censorship: Proposals for Responsible Delegation*, in *Va. J. Int'l L.* 2, vol. 60, 363-342, 2020.

[24] O. Pollicino, *Judicial protection of fundamental rights in the transition from the world of atoms to the word of bits: The case of freedom of speech*, in *European Law Journal* 2, vol. 25, 155-168, 2019.

[25] C. Unseld, *Horizontal Application*, in R. Grote, F. Lachenmann, R. Wolfrum, A. Harvey (eds.), *Max Planck Encyclopedia of Comparative Constitutional Law*, 2017,

the private ownership and management of these spaces of debate make it clear that envisaging a horizontal application of the principles enshrined in constitutional charters may be necessary to ensure that these actors do not consolidate an excessive opinion power[26].

Speech that is spread over social networking platforms is inherently transnational[27], as content is accessible almost everywhere on Earth (with the exceptions of countries where freedom of expression is severely curtailed by State institutions[28] or that suffer serious digital underdevelopment[29]). As a matter of fact, digital platforms that account for most users are generally incorporated in the USA, while still providing their services abroad, notably also to individuals located within – and subject to – the legal framework of the European Union and the Council of Europe. Despite appeals that have tried to induce a momentous change in attitude within the US legal community[30], the traditional scope of application of the Free Speech

<https://oxcon.ouplaw.com/view/10.1093/law-mpeccol/law-mpeccol-e308#>.

[26] The third-party effects of constitutional provisions ('Drittwirkung'), which implies that constitutional principles apply – albeit only indirectly ('mittelbare Drittwirkung') – to private legal relationship, developed within the German legal framework since the seminal *Lüth* decision (BVerfGE 7, 198, 15 January 1958), which dealt precisely with freedom of speech; see M. Borowski, *Drittwirkung*, in R. Grote-F. Lachenmann-R. Wolfrum-A. Harvey (eds.), *Max Planck Encyclopedia of Comparative Constitutional Law*, 2017, <https://oxcon.ouplaw.com/view/10.1093/law-mpeccol/law-mpeccol-e700>.

[27] J.L. Henn, *Targeting Transnational Internet Content Regulation*, in *B.U. Int'l L.J.* 1, in vol. 21, 157-178, 2003.

[28] J. Griffiths, *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*, Bloomsbury Publishing, London, 2021; B. Warf, *Geographies of global Internet censorship*, in *GeoJournal* 76, 1–23, 2011; R.J. Deibert, N. Villeneuve, *Firewalls and Power: An Overview of Global State Censorship of the Internet*, in M. Klang, A. Murray (ed.), *Human Rights in the Digital Age*, Routledge-Cavendish, London, 2004.

[29] J. Pierce, *Digital Divide*, in R. Hobbs, P. Mihailidis (eds), *The International Encyclopedia of Media Literacy*, Wiley-Blackwell, Hobonken (N.J.), 2019.

[30] E. Chemerinsky, *Rethinking State Action*, in *Northwestern University Law Review*, vol. 83, 3, 503-557, 1985-1986, who advocated for an apparently direct horizontal effect of constitutional guarantees for rights and liberties; S. Gardbaum, *The Horizontal Effect of Constitutional Rights*, in *Mich. L. Rev.* 3, vol. 102, 387-459, 2003, where the author advocates for the existence of an indirect horizontal effect of constitutional provisions, affecting the validity and the effectiveness of legislative rules regulating legal relationships between private parties; the above, however, rather than a nuance of the indirect *Drittwirkung* doctrine, appears an implied consequence of the understanding of the Constitution as the supreme law of the Land, whose violation may be sanctioned through the system of judicial review (Gardbaum itself makes reference to the Supremacy clause as the source that allows bypassing the State action threshold); a milder shift with respect to the traditional approach of US constitutional lawyers to horizontal effects

Clause of the First Amendment has been limited to conducts carried out by State institutions (*State action doctrine*)[31]. This means that, with notable exceptions where the judiciary has considered that activities operated by private entities fall within the category of functions traditionally within the exclusive domain of the State[32], there are no horizontal effects of constitutional provisions in the US legal system[33].

Acknowledging these remarkable differences is a key step to understand that any regulation of the channels through which online speech is disseminated must take into account the limits of State legislation in different legal systems and the extent to which platforms' providers may be held accountable for the policies of content moderation that they apply. A one-size-fits-all policy option is therefore very difficult to envisage, leaving stakeholders with a difficult conundrum to confront with. If convergence towards a common framework of regulation of platforms' accountability over content moderation is more desirable, the main avenue would probably encompass the devolution of most responsibilities to platforms themselves. This will imply reliance on their willingness to regulate speech so that an equitable balancing between needs to remove illicit content and risks of over-blocking[34] is struck. Nonetheless, self-regulation alone may arguably be sufficient to tackle effectively the phenomenon, thereby calling for more intrusive State intervention on the normative landscape; this, however, would likely pave the way for a jigsaw of different regulatory regimes depending on the given context and eventually difficult to reconcile one another.

Yet, under a European perspective, it is complicated not to consider

of constitutional provisions has suggested the introduction of a balancing judgment between the freedom of speech of the intermediaries and that of the users, see M. Yemini, *Missing in State Action: Toward a Pluralist Conception of the First Amendment*, in *Lewis & Clark L. Rev.* 4, vol. 23, 1149-1220, 2020, 1201.

[31] *United States v. Cruikshank*, 92 U.S. 542 (1875), in which the Supreme Court held that the Due Process Clause of the XIV Amendment applied as a limit only to federal legislation and not to legislation enacted by single States members to the Union. The decision in *Gitlow v. New York* (1925) eventually expanded the reach of the free speech clause of the I Amendment also to State legislation.

[32] *Marsh v. Alabama,* 326 U.S. 501 (1946); *Jackson v. Metropolitan Edison Co.*, 419 U.S. 345 (1974).

[33] G. Romeo, *Building Integration through the Bill of Rights: The European Union at the Mirror*, 47in *Ga. J. Int'l & Comp. L.*, vol. 47, 21-46, 2018, 40.

[34] S. Theil, *The German NetzDG: A Risk Worth Taking?*, *VerfassungsBlog*, 8 February 2018, <https://verfassungsblog.de/the-german-network-enforcement-act-and-the-presumption-in-favour-of-freedom-of-speech/>.

digital providers as actors similar to publishers of the traditional media, given the editorial control that they exercise over the content uploaded by users[35]. The difference lies in the method employed to shape the newsfeed presented to users. As each individual does not pick its own sources of information, if not through the interactions with content posted by other accounts and pages, it is the platform's algorithm that decides the priority order of the content appearing in the users' newsfeeds. More often than not, it is simplistic and down-to-earth content that circulates more quickly and, eventually, goes viral with no prior and due scrutiny that traditional media were supposed to carry out before going public with news. This mechanism implies an inherent bias towards undocumented stories and reports, thereby feeding the ever-increasing domain of inaccurate information (*fake news*) that fills the newsfeed of social media platforms[36].

3. *Free Speech and the Right to Be Informed: A Comparative Overview Between the European Multilevel and the US Constitutionalism*

This analysis requires two preliminary considerations. Firstly, the decision to tailor the scope of the research at the European supranational level, rather than at domestic ones, relies on the fact that this context of like-minded democracies, even in their cultural and legal differences, is equally challenged by technological transformation and it already presents a common ground of legal tools and shared constitutional sensitivities. Moreover, the European Union framework is jointly moving towards a unified approach to tackle digital constitutional challenges[37] and numerous

[35] S. Starinsky, *From Books to Facebook: How Social Media Became the Biggest Publisher of our Time*, in *Pub. Res. Q.* 37, 657–670, 2021, 663; the role of platforms has been deemed peculiar by those maintaining that there has been a shift from editorial control (typical of the traditional media) to organizational control (a feature of social media communication), see M.Z. van Drunen, *The post-editorial control era: how EU media law matches platforms' organisational control with cooperative responsibility*, in *Journal of Media Law* 2, vol. 12, 166-190, 2020.

[36] S. Vosoughi, D. Roy, S. Aral, *The spread of true and false news online*, in *Science* 359, 1146-1151, 2018.

[37] *Ex multis*, see *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan* COM/2020/790 final. See also the following proposals for Regulations: *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*

joint legislative efforts have been developed to regulate the anarchical vocation of the Internet[38]. Secondly, an analysis focusing exclusively on the European framework would be incomplete. A transatlantic perspective is needed given of the digital companies' tight link with Silicon Valley. An outline of the different constitutional sensitivities and of the regulatory efforts in their respective normative architectures will help to identify the similarities and divergences in strategic approaches on the two sides of the Atlantic, discussing whether joint efforts are ever possible.

From a methodological perspective, the analysis moves from a comparative investigation on the relevant legal basis in two legal frameworks, the US and the European one. The latter requires to take into considerations the multilevel complexity of overlapping legal systems – the Council of Europe and the European Union.

In the European panorama, the main constitutional standing of free speech is represented by Article 10 ECHR. Freedom of speech has been said to constitute the 'essential foundations of a democratic society'[39] and it stems from 'the demands of pluralism, tolerance and broadmindedness without which there is no «democratic society»'[40]. Yet, the implementation and enforcement of this right remain complex.

The structure of the provision tells something about the conventional status granted to such right, that is defined within the first paragraph which protects 'freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers'.

Freedom of expression is guaranteed to everyone, both natural and legal persons and no distinction is made with respect to the form of the expression – the Strasbourg Court recognised as falling within the scope of the provision the following: *e.g.* poem, brochure, photograph, or SMS[41].

Moreover, freedom of expression applies not only to the mere content,

2000/31/EC; *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; *Proposal for Regulation of the European Parliament and of the Council on the transparency and targeting of political advertising* COM/2021/731 final.

[38] On the Internet as a self-regulating platform, see P. Baran, *Communications, computers and people*, The Rand Corporation, Santa Monica, 1965.

[39] *Rekvényi v. Hungary* [GC], App no 25390/94, § 42, ECHR 1999-III.

[40] *Perinçek v Switzerland*, App no 27510/08 (ECtHR, 15 October 2015) § 196.

[41] See, respectively, *Karataş v. Turkey* [GC], App no 23168/94, § 49, ECHR 1999-IV; *Baran v. Turkey,* App no 48988/99, § 29, 10 November 2004; *Mosley v. United Kingdom*, App no 48009/08, § 115, 10 May 2011; *Bahçeci and Turan v. Turkey*, App no 33340/03, 16 June 2009.

but also to the channel through which expression is vehiculated; indeed, restrictions of these profiles interfere with the right to receive and impart information, which is expressly mentioned within the scope of the provision.

The second paragraph of the provision explicitly provides for a limitation clause, by mentioning the possibility to subject freedom of expression to 'formalities, conditions, restrictions or penalties'.

Firstly, possible restrictions of freedom of expression must be prescribed by law. Secondly, there must be a legitimate aim identified in the interests of national security, territorial integrity or public safety, as well as in the prevention of disorder or crime, the protection of health or morals, the protection of the reputation or rights of others, and in preventing the disclosure of information received in confidence, or in maintaining the authority and impartiality of the judiciary. Lastly, any restriction of freedom of expression must be necessary in a democratic society.

The explicit enumeration of legitimate aims to restrict freedom of expression highlighs that the protection is not granted an absolute status within the European panorama[42]. Even if the scope of the provision grants freedom of expression the value of a fundamental right, it also leaves Member States a wide margin of appreciation[43] as to possible derogations deemed necessary in a democratic society[44].

The Strasbourg Court has repeatedly stated that such restrictions are to be constructed in stringent terms[45] and the need for such limitations must be 'established convincingly'[46].

The rise of the Internet has implied the necessity to rethink the analysis and interpretation of Article 10 ECHR. The European Court of Human Rights (ECtHR) has protractedly interpreted the Convention as a living

[42] J.-F. Flauss, *The European Court of Human Rights and the Freedom of Expression*, in *Ind. L.J.* 3, vol. 84, 809-850, 2009.

[43] On doctrine of the margin of appreciation – which has been developed from the case *Handyside v. United Kingdom* (ECtHR, 7 December 1976) – see M.R. Hutchinson, *The Margin of Appreciation Doctrine in the European Court of Human Rights*, in *International & Comparative Law Quarterly* 3, vol. 48, 638-650, 1999.

[44] D. Voorhof, *Freedom of Expression under the European Human Rights System. From Sunday Time (no 1) v U.K. (1979) to Hachette Filipacchi Associès ('Ici Paris') v France (2009)*, in *Inter-American and European Human Rights Journal* 3, vol. 1-2, 2009; F. Tulkens, *Freedom of expression and hate speech in the case-law of the European Court of Human Rights* in J. Casadevall, E. Myjer, M. O'Boyle (eds), *Freedom of Expression. Essays in Honour of Nicolas Bratza* (Wolf Legal Publishers 2012).

[45] *Stoll v. Switzerland* [GC], App no 69698/01, § 61, ECHR 2007-V.

[46] *Janowski v. Poland* [GC], App no 25716/94, § 30, ECHR 1999-I; *Nilsen and Johnsen v. Norway* [GC], App no 23118/93, § 43, ECHR 1999-VIII.

instrument[47], whose interpretation needs to be in line with present-day legal culture and sensitivities. In light of such an interpretative path, it is important to stress the Strasbourg Court's understanding of the pivotal role of the Internet 'in enhancing the public's access to news and facilitating the dissemination of information in general' as well as the central function of user-generated contents online as 'an unprecedented platform for the exercise of freedom of expression'[48].

At the same time, in the Court's reasoning, the Internet has also amplified potential risks for other fundamental rights[49], thereby arguing for the necessity to rethink the balancing test between freedom of expression and other fundamental rights in light of the peculiarities of the digital dimension.

The right to freedom of expression and information is positively recognized also at the European Union level by Art. 11 of the Charter of Fundamental Rights of the EU (CFR), which echoes Art. 10 ECHR. Even if, as explicitly provided by Article 52(3) CFR, the meaning and scope of the two provisions are the same[50], Art. 11(2) CFR exceeds the scope of application of Art. 10 ECHR by providing explicitly that media freedom and pluralism have to be respected.

On its active nuance, Article 11(1) CFR protects the right to hold an opinion and the possibility to communicate it, regardless the form of expression, the means of communication through which it is vehiculated, and its content[51]. Moreover, it also covers the negative side in the form of the right not to express one's opinion.

Art. 11 CFR also implies the protection of a passive nuance, by explicitly

[47] G. Letsas, *The ECHR as a living instrument: its meaning and legitimacy*, in A. Føllesdal, B. Peters, G. Ulfstein (eds.), *Constituting Europe. The European Court of Human Rights in a National, European and Global Context*, Cambridge University Press, Cambridge, 2013.

[48] *Cengiz and Others v. Turkey*, App no 48226/10, 1 December 2015, § 52; *Ahmet Yildirim v. Turkey*, App no 3111/10, 18 December 2012, para. 48; *Times Newspapers Ltd v. the United Kingdom* (nos. 1 and 2), App nos 3002/03 and 23676/03, 10 March 2009, § 27.

[49] *Editorial Board of Pravoye Delo and Shtekel v Ukraina*, App no 33014/05 (ECtHR, 5 May 2011).

[50] For role of the European Convention on Human Rights (ECHR) in the interpretation of the Charter of Fundamental Rights, see G. Gaja, *The Charter of Fundamental Rights in the Context of International Instruments for the Protection of Human Rights*, in *European Papers* 3, vol. 1, 791-801, 2016.

[51] See also L. Woods, *Article 11*, in S. Peers T. Hervey, J. Kenner, A. Ward (eds.), *The EU Charter of Fundamental Rights: A Commentary*, Bloomsbury Publishing, London, 2014.

mentioning the freedom to receive information and ideas[52], making the shaping of individual opinions a precondition to fully exercise freedom of expression. The right to receive information is especially relevant for media regulation and for advertising.

The distinguishing element between the two European provisions is that Art. 11 CFR expressly deals with media, acknowledging the necessity, in a democratic society, for a variety of free media. Freedom, on one side, and pluralism, on the other, are the main pillars on which the protection provided for by Article 11(2) CFR is declined. The provision states that media shall enjoy freedom of expression, which protects communication outlets as loudspeaker of opinions and ideas, whereas media pluralism[53] recognizes the necessity that Member States ensure potential accessibility to a variety of different media. While the former is considered a subjective right, the latter has been recognized by the Luxembourg Court as a legitimate policy aim[54], leaving it ambiguous whether Art. 11(2) CFR encompasses a distinct subjective right to media pluralism or whether the latter is a public policy objective and interpretative aid.

Freedom of expression has also been recognized as one of the essential foundations of democratic pluralistic societies by the CJEU[55], yet it is not an absolute right. Unlike Art. 10(2) ECHR, which explicitly mentions limitations to such right, the CFR provides for general restrictions to a series of rights in Art. 52(1) and 52(3).

In general terms, the limitations of freedom of speech shall be restrictively interpreted and any assessment shall be addressed in light of the type of speech as well as its content[56].

Borrowing from the ECtHR's approach, the extent to which restrictions are admissible depends on two reasons. The first step requires to verify whether the limitation seeks a legitimate aim. In this sense, the Luxembourg Court has outlined the overriding interests for the Treaty freedoms as an open class. Yet, it is proposed that acceptable grounds within the scope of this provision cannot be wider than those provided for

[52] Case C-477/10, *Commission v Agrofert Holding*.

[53] For an assessment of media pluralism within the scope of Article 11 CFR, see P. Cavaliere, *An Easter egg in the Charter of fundamental rights: The European Union and the rising right to pluralism*, in *International Journal of Public Law and Policy* 4, vol. 2, 357-396, 2012.

[54] Case C-288/89, *Gouda*, § 23.

[55] Joined Cases C-203/15 & C-698/15, *Tele2 Sverige*, § 93.

[56] *The Sunday Times v. United Kingdom*, ECtHR, App no 6538/74, 26 April 1979; *Patriciello* Case C-163/10, Judgment of the Court (Grand Chamber) of 6 September 2011.

by Art. 10(2) ECHR. Those fields in which EU legal rules intervene to restrict speech (*e.g.*, regulation of advertising) are likely to fall within those grounds allowing for restrictions on matters of public concern or public interest. The second step is the assessment of proportionality balancing the relevance of any countervailing interests.

The analysis of the constitutional framework on freedom of speech on the other side of the Atlantic shall start with an assessment of the First Amendment, which states that 'Congress shall make no law […] abridging the freedom of speech, or of the press'. The negative formulation in the wording of the First Amendment reveals the primary concern of prohibiting State powers to interfere with the exercise of free speech, which has effects in the development of the concrete guarantees provided to this right[57]. Therefore, as stated by Justice Black, a textualist approach guides on considering the First Amendment according to its literal meaning, thereby interpreting 'shall make no laws' and 'abridging' as an impossibility for federal, State, and local governments to restrict free speech[58].

Possible limitations that do not contravene the scope of the First Amendment have been developed by the judicial formant[59]. On one side, content-based restrictions have been recognized for those categories of speech that have limited social standing. On the other side, limitations have been recognized on expressions directed at inciting conducts. US constitutional law deploys three categories of speech, differentiated basing on its content[60]. Aside from high-value speech, whose core is related to topics of public interest (political speech), there are the intermediate-value speech, primarily concerned with commercial speech and similar advertising, and low-value speech, such as for example vulgarity and libellous expressions[61]. The constitutionality of a regulation providing restrictions of the first kind is subject to strict scrutiny, meaning that it is necessary to detect that the

[57] M. Tushnet, *Advanced Introduction to Freedom of Expression*, Edward Elgar Publishing, Cheltenham–Northampton (MA), 2018, 22; T.I. Emerson, *The System of Freedom of Expression*, Random House, New York, 1970; T.I. Emerson, *Toward a General Theory of the First Amendment*, in *Yale Law Journal*, vol. 72, 877 ff. (1963); R.J. Krotoszynski, *The Disappearing First Amendment*, Cambridge University Press, Cambridge, 2019.

[58] *Barenblatt v the United States*, 360 U.S. 109, 143–44 (1959); *Smith v California*, 361 U.S. 147, 157 (1959).

[59] R. Sacco, *Legal formants: a dynamic approach to comparative law (Installment I of II)*, in *The American Journal of Comparative Law* 1, vol. 39, 1-34, 1993.

[60] G.R. Stone, *Content Regulation and the First Amendment*, in *William and Mary Law Review* 2, vol. 25, 189-252, 1983.

[61] M. Tushnet, *Advanced Introduction to Freedom of Expression*, Edward Elgar Publishing, Cheltenham–Northampton (MA), 2018, 22.

restriction is justified by a strong or compelling public interest that cannot be equally protected through less restrictive means. On the contrary, intermediate scrutiny is sufficient to assess restrictions of the second type of speech, verifying the presence of a major public interest in the limitation, and that the latter directly and proportionally pursues the interest; this assessment shall be carried also in light of other available possibilities. Finally, the test for assessing restrictions of low value speech is carried with the scrutiny of reasonability (rational basis test).

This approach is different from the European one and it stems both from the position accorded to free speech in the US panorama and the traditional liberal view surrounding it: free speech has been accorded a quasi-absolute position[62] as 'the paramount right within the American constellation of constitutional rights'[63]. The interpretation of the US Supreme Court, which recognizes to freedom of speech a crucial role within the US constitutional architecture, focuses on the active nuance of free speech, and it is addressed at preventing the government from limiting protected speech. Legitimate restrictions in public forums must comply with strict scrutiny. Nonetheless, the dimension of constitutional protection under the First Amendment has also shifted to focus on the audience's right to receive information[64]. In this view, access to information is a precondition and component of the right to free speech, arguing that the latter is empty without the former.

While in the European panorama the analysed provisions explicitly provide for a right to be informed, this passive dimension is not encompassed within the First Amendment's wording, and it has emerged only through the Supreme Court's interpretation. The first case in which the US Supreme Court addressed access to information were *Martin v. Struthers* and *Thomas v. Collins*[65], where the Justices underlined the importance of access to information as a necessary correlative for the protection of the free speech. The connection between free speech and access to information

[62] F. Schaurer, *Freedom of Expression Adjudication in Europe and America: A Case Study in Comparative Constitutional Architecture*, in G. Nolte (eds.), *European and US Constitutionalism*, Cambridge University Press, Cambridge, 2005, 49 ff.
[63] M. Rosenfeld, A. Sajó, *Spreading Liberal Constitutionalism: An Inquiry into the Fate of Free Speech Rights in New Democracies*, Cardozo Legal Studies Research Paper No 144 (2005), available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=870444>.
[64] W.E. Lee, *The Supreme Court and the Right to Receive Expression*, *The Supreme Court Review*, 303-306 (1988).
[65] *Martin v. Struthers*, 319 U.S. 141, 143 (1943); *Thomas v. Collins*, 323 U.S. 515, 534 (1944).

has been a crucial point in the development of the Court's interpretation over the First Amendment. In one of the cases on free speech concerning post offices retaining foreign communist mailings[66], Justice Brennan discussed the connection among free speech and access to information, arguing that '[i]t is true that the First Amendment contains no specific guarantee of access to publications. However, the protection of the Bill of Rights goes beyond the specific guarantees to protect from congressional abridgment those equally fundamental personal rights necessary to make the express guarantees fully meaningful […]. The dissemination of ideas can accomplish nothing if otherwise willing addressees are not free to receive and consider them. It would be a barren marketplace of ideas that had only sellers and no buyers'[67].

In *Stanley v. Georgia*[68], the Court stated that by then it was 'well established that the Constitution protects the right to receive information and ideas', and also the right to receive indecent material was to be protected under the scope of the First Amendment. The US Supreme Court later built on the principle to justify protection for commercial speech in *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council*[69], highlighting the right of the public to receive information on prices for prescription drugs. However, it was in *Board of Education v. Pico*[70] that the Court explained that the right to receive information and ideas is important for both free speech and free press. On one hand, the right to receive information stems directly from the right to express or disseminate them[71]. On the other, it is 'a necessary predicate to the recipient's meaningful exercise of his own rights of speech, press, and political freedom'[72].

[66] *Lamont v. Postmaster General*, 381 U.S. 301 (1965).
[67] *Lamont v. Postmaster General*, 381 U.S. 301, 308 (1965).
[68] 394 U.S. 557 (1969).
[69] 425 U.S. 748 (1976).
[70] *Board of Education, Island Trees Union Free School District No 26 v. Pico*, 457 U.S. 853 (1982).
[71] *Lamont v. Postmaster General*, 381 U.S. 301 (1965).
[72] *Board of Education, Island Trees Union Free School District No 26 v. Pico*, 457 U.S. 853 (1982).

4. *The Phenomenon of Political Micro-Targeting Which Regulation to Safeguard Democratic Processes?*

The Internet poses numerous challenges to the regulation of the democratic public sphere[73], and specifically to the paradigm of protection of freedom of expression. In the online dimension, the possibility for digital platforms to gather users' data showing their inner preferences has shaped a profitable business model, which is powered by the maximisation of users' entertainment in digital and social networking meanders. The more users are connected, the more data are collected, the more personal profiles are accurate, resulting in the rise of online ads fees, which makes it possible to offer a free or low-cost service.

Digital platforms monetise from users' engagement, personal preferences, political orientations and emotional vulnerabilities, which is only possible through the access and scanning of every bit of data[74]. This model locks users within digital cages, in which they are exposed to different phenomena. Firstly, on the basis of browsing history and personal information, algorithms function in a way that leaves users within a *filter bubble*, where they are exposed exclusively to contents and news that share their opinions and biases[75]. These mechanisms do not always operate and function transparently[76], thereby leaving outside content that holds contrary or that challenges the main ideas within the echo chamber, which results in polarizing

[73] To the purposes of this research, public sphere shall be intended as the Habermasian ideal of a dialogic dimension on public matters, see J. Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into Category of Bourgeois Society*, Polity, Cambridge, 1989 [1962].

[74] The unbridled access to users' data poses serious challenges on privacy and on the protection of personal data. These concerns for the end-user have been extensively discussed from different point of views. Though it is not intended to be the focus of the present paper, for such discussions see, *ex multis*, I.S. Rubinstein, *Voter Privacy in the Age of Big Data*, in *Wisconsin Law Review* 5, vol. 1, 861-936, 2014; C.J. Bennett, *Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications*, in *Surveillance and Society* 3/4, vol. 13, 370-384, 2015.

[75] E. Pariser, *The Filter Bubble: What the Internet is Hiding From You*, London-Viking, Penguin, 2011.

[76] Academic scholars have extensively studied the functioning of algorithmic technologies, often raising concerns over algorithmic discriminatory biases. See F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge (MA), 2015; A. Chander, *The Racist Algorithm?*, in *Michigan Law Review* 6, vol. 115, 1023-1046, 2017; S.U. Noble, *Algorithms of Oppression. How Search Engines Reinforce Racism*, New York University Press, New York, 2018.

the opinions of those that are locked within the network[77].

Secondly, modern campaigns are increasingly exploiting the possibility to efficiently diversify their messages and to tailor them on the voter's personal preferences, permitting to focus on certain voters or geographical areas[78] with a saving in cost and time. Targeting voters enables not only to personalise the content of the message, but to communicate it using the most familiar language and to vehiculate it through the most used social media.

These phenomena tend to sharpen trajectories of political polarization[79], which may fuel extremist movements and undermine the foundations necessary for a political regime that demands acceptance and compromise between different political forces[80]. Moreover, they are intensified in electoral and referendum campaigns[81], in which a tendency to polarization[82] is to some extent physiological and not necessarily pathological.

Firstly, in nowadays online political arenas, parties and candidates that have greater financial resources have higher chances to access to micro-targeting services, either to create messages favourable to themselves or to oppose those put forward by their political competitors. Secondly, polarization tends to divert voters' attention from the political program, transforming what should be a rational choice into mere adhesion. Finally, when political propaganda is so fierce as to resort to false information, the same disinformation is repeatedly shared in echo chambers, increasing the perception of its accuracy[83]. In these media ecosystems, the compromise between different instances and sensitivities, which in a democratic regime should be physiological, ends up being perceived by the electorate as a betrayal, powering attitudes of disaffection[84].

---

[77] C.R. Sunstein, *#Republic. Divided Democracy in the Age of Social Media*, Princeton University Press, Princeton-Oxford, 2017, 59 ff.

[78] D.W. Nickerson, T. Rogers, *Political Campaigns and Big Data*, in *Journal of Economic Perspectives* 2, 51–74, vol. 28, 2014.

[79] For the problems of social fragmentation, see C.R. Sunstein, *Republic.com*, Princeton University Press, Princeton (NJ), 2002; C.R. Sunstein, *Republic.com 2.0*, Princeton University Press, Princeton (NJ), 2007.

[80] H. Kelsen, *The Essence and Value of Democracy*, Rowman & Littlefield Publishers, Lanham (MD), 2013 [1920].

[81] C.J. Bennett, D. Lyon, *Data-driven elections: implications and challenges for democratic societies*, in *Internet Policy Review* 4, 1-16, vol. 8, 2019.

[82] C.R. Sunstein, *Designing democracy: what Constitutions do*, Oxford University Press, New York, 2001.

[83] Y. Benkler, R. Faris, H. Roberts, *Network propaganda: manipulation, disinformation, and radicalization in American politics*, Oxford University Press, New York, 2018.

[84] The existence of citizens' political apathy is a symptom of the perceived inability of

Digital communication dynamics can produce a distorting effect over public opinion's building processes that, in democratic pluralistic societies, should be shaped through the confrontation of a variety of opinions and ideas, making the dialectic competition an essential feature. The formation of the public opinion within the online environment is distorted at two distinct, yet complementary levels. On the individual level, the dynamics shaping voters' opinions on electoral programs and on political incumbents' actions tend to be influenced by the majority's orientations, and even more by those ideas prevailing within the group to which the individual voter belongs and identifies with. Locking the voter within an echo chamber may only strengthen existing ideas shared and reinforced among the group.

On the collective level, public opinion can be seen as the result of a dialectical confrontation among different individual opinions over issues of common interest, which can be hindered by different dynamics. On one hand, the Net leads, and subsequently locks, users within specific meanders of its structure, exposing them only to certain contents. On the other, relevant political issues are vehiculated only to certain users, hetero-directed towards them by private actors through digital platforms' infrastructures.

While quantifying these phenomena's concrete impact on democracy may be a difficult exercise, the potential threats have materialized in the events concerning Facebook and Cambridge Analytica, which have revealed the potentially disruptive effects on the democratic whole and the impact over fairness and transparency of electoral and referendum processes[85]. Being aware of the possibilities of manipulation of electoral consensus[86] and of the alteration of equal opportunities of the actors involved in the political game seems necessary to address these constitutional challenges[87].

representative institutions to grasp the numerous social demands, developing into a form of disaffection to voting, also as a consequence of the crisis of political parties. This circumstance, on the other hand, has also led to forms of populist reaction and mobilization. These are recurrent *topoi* in constitutional and political debates. On the decreasing engagement between political parties and citizens, see G. Klaukka, S. van der Staak, J. Valladares, *The changing nature of political parties and representation*, in *International Institute for Democracy and Electoral Assistance*, *The Global State of Democracy: Exploring Democracy's Resilience*, Stockholm, International IDEA, 2017, 98–118.

[85] F.J. Zuiderveen Borgesius, J. Möller, S. Kruikemeier, R. Ó Fathaigh, K. Irion, T. Dobber, B. Bodo, C. de Vreese, *Online political microtargeting: Promises and threats for democracy*, in *Utrecht Law Review* 1, vol. 14, 82-96, 2018.

[86] J. Burkell, P.M. Regan, *Voter preferences, voter manipulation, voter analytics: policy options for less surveillance and more autonomy*, in *Internet Policy Review* 4, vol. 8, 1-24, 2019.

[87] H.W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G.

These challenges are not new to the offline world. Yet, their effect could exert a totally different impact in the online dimension; indeed, it has proven difficult to make electors immune from evident or concealed attempts of hetero manipulation.

Online political micro-targeting poses challenges to the regulation of a democratic public sphere, impacting the citizens' right to be informed. With regard to the EU panorama, the potential interference of online political micro-targeting with the right to receive information, expressly outlined within the scope of Article 11 CFR, is apparent. Different considerations have to be made in this regard. Firstly, Article 11 CFR is applicable only for political micro-targeting strategies implied in the context of the EU Parliament's elections. Indeed, Article 51(1) CFR states that the Charter's provisions are binding on Member States only when they are implementing EU law. The CJEU has notably stated that the fundamental rights guaranteed in the EU legal order are applicable only in circumstances that are governed by EU law, and it has denied its jurisdiction for the examination of the compatibility with the Charter of national legislation that falls outside the scope of EU law[88]. This is another important reason that justifies the analysis of the Council of Europe framework, given the applicability of the ECHR in national elections. Secondly, a literal interpretation of Article 11 CFR implies to question whether private actors – such as political parties and platforms – could be considered within its scope of application[89], given that the provision only prevents public authorities' interferences. The CJEU has not yet confronted with the issue on whether political micro-targeted ads could fall within the scope of application of the Nice Charter's provision.

With regard to Article 11 CFR, the Luxembourg Court's approach has developed into a different direction, tackling issues regarding the balancing

De Gregorio (eds.), *Constitutional Challenges in the Algorithmic Society*, Cambridge University Press, Cambridge UK, 2021.

[88] Case C-617/10, *Åklagaren v Hans Åkerberg Fransson*.

[89] Valuable scientific research has already answered this question, «arguing that there are four possible ways to overcome this lacuna in legal protection: (i) rejecting horizontal direct effect of this provision and relying on secondary legislation; (ii) recognising horizontal direct effect of this provision; (iii) imposing a positive obligation on Member States to protect this fundamental right; and (iv) recognising quasi-public powers of the abovementioned private parties in order to turn a horizontal relationship into a vertical one». See M. Brkan, *EU fundamental rights and democracy implications of data-driven political campaigns*, in *Maastricht Journal of European and Comparative Law* 6, vol. 27, 774-790, 2020, 778; M. Brkan, *Freedom of Expression and Artificial Intelligence: On Personalization, Disinformation and (Lack Of) Horizontal Effect of the Charter*, Maastricht Faculty of Law Working Papers, 9, 2019.

between freedom of expression and information and copyright[90], between freedom of expression and information and broadcasting rights[91], freedom of expression and information and the labelling of products[92], or the advertising of products[93].

Within the EU framework, online advertising is being specifically tackled with several acts, namely the *Digital Services Act* (DSA), the European Democracy Action Plan, and the EU legislators' proposed Regulation on transparency and targeting for political advertising. While by regulating digital marketing and issues-based advertising, complementing the GDPR, the first aims at ensuring an online environment shaped as safe and accountable, the second is aimed at empowering citizens and democracies in the EU, by supporting free and fair elections, guaranteeing transparency of online advertising, strengthening media freedom, and responding to disinformation issues. Lastly, building on the requirement for any political ad to be clearly labelled, the proposal for Regulation on transparency and targeting for political advertising aims to create a safer environment for the processing of users' personal data.

Within the Council of Europe framework, political micro-targeting has not been specifically examined yet by the Strasbourg Court. However, in a case of 2008 concerning a political party paying for a TV advertisement during an electoral campaign[94], the Court held that such a conduct is a form of political speech, which enjoys the highest protection under Article 10. Given the similar rationale, also political micro-targeting through social media may fall under Article 10 ECHR, the consequence being the application of a strict scrutiny in the evaluation of any potential restriction of its dissemination[95]. In other words, if micro-targeting is seen as political speech, the protection granted under Article 10 makes it difficult to restrict it, as the compatibility of potential limitations needs to be addressed with regard to different stakeholders' instances, such as the political party's[96] or an elected representative's[97] freedom of expression.

The Strasbourg Court's case law has underlined that Article 10

[90] Case C-360/10, *SABAM*; Case C-70/10, *Scarlet Extended*; Case C-516/17, *Spiegel Online*; Case C-469/17, *Funke Medien NRW*; Case C-160/15, *GS Media*.
[91] Case C-283/11, *Sky Österreich*.
[92] Case C-547/14, *Philip Morris Brands and Others*; Case C-157/14, *Neptune Distribution*.
[93] Case C-421/07, *Damgaard*.
[94] *TV Vest v. Norway*, no 21132/05 (ECtHR, 11 December 2008).
[95] *TV Vest v. Norway*, no 21132/05 (ECtHR, 11 December 2008).
[96] *Magyar Kétfarkù Kutya Pàrt v. Hungary*, App no 201/17 (ECtHR, 23 January 2018).
[97] *Otegi Mondragon v. Spain* App no 2034/07 (ECtHR, 15 March 2011).

protects politicians and political parties' freedom of expression from a two-fold perspective: firstly, as an important tool to represent and defend the electorate's interest[98]. Secondly, the Court linked this protection with the positive consequences on democracy itself[99]. As it has been explained, political speech does not amount to an absolute right, and it can be restricted on certain conditions. The ECtHR's judicial approach of political advertising in broadcasting gives good indications on how the Court would assess online political micro-targeting. The Strasbourg Court has explained the grounds on which political speech may be subject to restrictions «aimed at supporting the integrity of the democratic process, to obtain a fair framework for political and public debate, and to avoid a situation where those who could afford it obtained an undesirable advantage by using the most potent and pervasive medium»[100].

The deterrence of distortion of the electoral process[101] and the electorate's right to a balanced and impartial information[102] have been accepted as legitimate aims within the ECHR framework. This gives the perception that acts infringing these values result in a violation of voters' fundamental rights, whose role for the democratic process is pivotal. Thus, it could be argued that leaving its safeguards to platforms' algorithmic discretion is detrimental to voters' fundamental rights and, as a consequence, to democracy itself. The existing judicial approach is not sufficient to foresee whether targeted political advertising would be considered legitimate, yet it gives the measure of the importance of a balancing process between competing interests and of the necessity to determine potential justificatory grounds for the limitation of political parties' freedom of expression[103].

With regard to national rules on political micro-targeting in Europe, France presents a strict framework. Pursuant to Article L. 52-1 of the Electoral Code[104], the use of any commercial advertising process for election propaganda purposes in the press or any source of audio-visual communication, including online public communication, is prohibited[105].

[98] *Castells v. Spain* App no 1798/85 (ECtHR, 23 April 1992).
[99] *United Communist Party of Turkey v. Turkey* App no 19392/92 (ECtHR, 30 January 1998).
[100] *TV Vest v. Norway* App no 21132/05 (ECtHR, 11 December 2008) § 44.
[101] *Erdoğan Gökçe v. Turkey* Apps nos 346/04 and 39779/04 (ECtHR, 27 May 2014).
[102] *Orlovskaya Iskra v. Russia* App no 42911/08 (ECtHR, 21 February 2017).
[103] M. Brkan, *EU fundamental rights and democracy implications of data-driven political campaigns*, in *Maastricht Journal of European and Comparative Law* 6, vol. 27, 774-790, 2020, 778.
[104] Article L52-1, *Code électoral*.
[105] A. Granchet, *France*, in M. Cappello (eds.), *Media coverage of elections: the legal*

Moreover, the Law no 2018-1202 of 22 December 2018 on countering information manipulation has amended the *Code electoral* by introducing Article L. 163-1, which states that operators of online platforms[106] shall provide users with fair, clear and transparent information on the identity of who commissioned and paid for the advertisements vehiculating a content related to a public interest debate. This disclosure mandate applies only during the three months before the month in which national general elections are held.

As it has been explained by the *Conseil Supérieur de l'Audiovisuel* (CSA), information content related to a public interest debate includes every issue that affects the public so that the latter has a reasonable interest in it, notably because it concerns the well-being of citizens or of the community[107].

The French approach is important in light of two considerations. On one hand, there seem to be an information-fiduciary approach, which resembles the one that the EU is adopting (see *Regulation on transparency and targeting for political advertising*). On the other, though, the French framework permits to observe the implementation of such a legislative approach, which has led to the decision by some platforms to completely prohibit political campaigning and issue advocacy advertisements[108].

In Germany, the regulation of election advertising widely varies among broadcasters, printed and online media[109]. Within this latter category further distinction shall be made among online broadcasting and telemedia, such as social media platforms and on demand services.

The online transmission of a programme according to a schedule

framework in Europe, Strasbourg, European Audiovisual Observatory, 2017, 29–37.

[106] The definition of platform operators is the provided for in Article L. 111-7 of the French Consumer Code.

[107] *Recommandation n. 2019-03 du 15 mai 2019 du Conseil supérieur de l'audiovisuel aux opérateurs de plateforme en ligne dans le cadre du devoir de coopération en matière de lutte contre la diffusion de fausses informations*.

[108] Microsoft. (2019). Disallowed content policies. Retrieved from https://about.ads.microsoft.com/en-us/resources/policies/disallowed-content-policies
Google (2019a). Political content. Retrieved from https://support.google.com/adspolicy/answer/6014595?hl=en ; Google (2019b). An update on our political ads policy. Retrieved from https://blog.google/technology/ads/update-our-political-ads-policy/
Twitter (2019a). Political Content in the European Union. Retrieved from https://business.twitter.com/en/help/ads-policies/restricted-contentpolicies/political-content/eu-political-content.html
Twitter (2019b). Political Content. Retrieved from https://business.twitter.com/en/help/adspolicies/prohibited-content-policies/political-content.html

[109] C. Etteldorf, *DE – Germany*, in M. Cappello (eds.), *Media coverage of elections: The legal framework in Europe*, European Audiovisual Observatory, 2017, 30, 37.

(*e.g.* live streaming services) is classified as broadcasting and, as such, it is subject to the provisions applicable to election advertising in broadcasting: Article 7(9)(1) of the *Rundfunkstaatsvertrag* (Inter-State Broadcasting Agreement, *RStV*) provides for the prohibition of paid political advertising in broadcasting during election campaigns. Broadcasting outlets have the obligation to assign free airtime to parties for electoral advertising.

On the contrary, if the content is simply vehiculated through the Internet, it will fall within the category of telemedia, which is regulated by Articles 54 et seq. *RStV*. Article 58(3)(1), read in conjunction with Article 7(9) of the *RStV*, prohibits election advertising via on-demand audiovisual media services. However, social media platforms are not included within the scope of application of these provisions.

Contrary to the French approach, the German one appears to be more lenient toward the regulation of online advertising, that is left to self-regulation. This feature differs also from the German approach towards broadcasting and printed media which are extensively regulated.

5. *Comparative approaches to political disinformation, false statements and online advertisement*

The identification of the legislative and judicial approaches to disinformation in politics requires a preliminary assessment of the nature of the phenomenon and the mechanisms underlying its extraordinary spread. There is no conclusive agreement in legal scholarship or among operators of the informational market on what exactly fake news are and to what extent objectively false content shall be censored or removed from digital platforms. One point of convergence seems the consideration that this content must cause harm to some of the recipients[110]. Reference to the intentional dissemination of news that a speaker is aware that is not true is thus pivotal to set the boundaries of this issue[111]. Therefore, only disinformation campaigns specifically addressed at circulating news not believed to be true even by those disseminating it would qualify as fake news. This includes political statements by candidates running for an elective office that contain information that the speaker circulates despite

[110] R. Ó Fathaigh, N. Helberger, N. Appelman, *The perils of legally defining disinformation*, in *Internet Policy Review*, 10(4), 2021.

[111] B. Baade, *Fake News and International Law*, in *European Journal of International Law*, vol. 29, Issue 4, November 2018, 1357–1376.

the knowledge about its falsity. On the contrary, the dissemination of news that, while objectively false, is believed in good faith to be true would rather fall within the category of misinformation[112].

The mechanisms that allow for the spread of fake news and drive the success of disinformation campaigns overlap to many extents to those that enable micro-targeted political campaigns (see §4); more specifically, disinformation patterns proliferate in the context of digital infrastructures enhancing the consolidation of echo chambers. In these environments, the news presented to the user is not tested against opposing or negotiating views, thus increasingly persuading him or her of its truth and making it more likely that he or she shares the content. Indeed, content shared by acquaintances is more likely to be believed true than news coming from neutral third parties or unknown users[113].

Disinformation campaigns bring about at least a twofold risk. First, by encouraging users of social networking platforms to lock themselves into filter bubbles, they fuel the dynamics of political polarisation (see §4); the latter threatens the willingness to compromise in policy choices and, eventually, might lead either to paralysis in State administration or to uncontrolled abuse by majorities against minority groups. Second, the inexistence of solid barriers towards the dissemination of false statements and inaccurate information makes modern democratic systems vulnerable to potential concerted efforts by foreign States[114] aimed at undermining the trust of the public opinion in democratic processes and influencing electoral outcomes[115].

The relevance of the phenomenon is not underestimated in the European environment. The EU strategy to tackle disinformation in the online environment could be divided into two strands. Originally, the fight against the manipulation of information online has been directed at ensuring the fairness of electoral and democratic processes, reminiscent

[112] *The legal framework to address "fake news": possible policy actions at the EU level*, Policy Department for Economic, Scientific and Quality of Life Policies Author: Andrea Renda (CEPS - Centre for European Policy Studies and College of Europe), Directorate-General for Internal Policies, PE 619.013- June 2018, 5.

[113] C. Wardle, H. Derakhshan, *Information Disorder. Toward an interdisciplinary framework for research and policymaking*, September 27, 2017, Council of Europe report DGI(2017)09.

[114] R. Ó Fathaigh, T. Dobber, F.J. Zuiderveen Borgesius, J. Shires, *Microtargeted propaganda by foreign actors: An interdisciplinary exploration*, in *Maastricht Journal of European and Comparative Law* 6, vol. 28, 856-877 2021.

[115] S. McKay, C. Tenove, *Disinformation as a Threat to Deliberative Democracy*, in *Political Research Quarterly* 3, vol. 74, 703-717, 2021.

of the outcome of the campaigns for the 2016 Brexit referendum and US Presidential elections. After the Covid-19 pandemic, the concern of EU institutions seems to have shifted, at least to some extent, towards the identification of effective strategies to curtail the spread of inaccurate medical information (*e.g.*, anti-vaccination campaigns)[116].

Yet, up until the most recent proposals for regulation of the digital market (see §6), the efforts undertaken by EU institutions had stopped short of introducing relevant instruments of legislation with binding effects. The fight against disinformation in the EU has been built around an online public consultation[117], a EuroBarometer report[118] and a Report of the High-Level Group instituted by the European Commission[119], which supplement a specific communication issued by European Commission in 2018[120]. The closest the EU had come to a binding instrument of law until 2022 was the EU Code of Practice on Disinformation, which was opened to signature from members of the digital industry as a self-regulation tool encompassing some of the conclusions of the above soft law instruments[121]. Interestingly, the intention to prevent damages to the integrity of democratic processes is one of the drivers of the adoption of a communication establishing election cooperation networks aimed at ensuring the fairness of the processes underlying the 2019 elections of the European Parliament[122].

As the Code of practice was eventually gaining traction following

[116] R. Harrison, *Tackling Disinformation in Times of Crisis: The European Commission's Response to the Covid-19 Infodemic and the Feasibility of a Consumer-centric Solution*, in Utrecht Law Review 3, vol. 17, 18–33, 2021.

[117] *Synopsis report of the public consultation on fake news and online disinformation*, Consultation Results, 26 April 2018, https://digital-strategy.ec.europa.eu/en/synopsis-report-public-consultation-fake-news-and-online-disinformation.

[118] *Fake news and disinformation online*, Flash EuroBarometer 464 Report, 27 April 2018, https://op.europa.eu/en/publication-detail/-/publication/2d-79b85a-4cea-11e8-be1d-01aa75ed71a1.

[119] *A multidimensional approach to disinformation*, Report of the independent High-level Group on fake news and online disinformation, 30 April 2018, https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1.

[120] *Tackling online disinformation: a European Approach*, COM(2018) 236, 26 April 2018.

[121] *EU Code of practice on disinformation*, September 2018, which has yet to enter into force with binding effects; see also C. Marsden, T. Meyer, I. Brown, *Platform values and democratic elections: How can the law regulate digital disinformation?*, in *Computer Law & Security Review* 36, 2020.

[122] C(2018) 5949 final, Commission recommendation of 12.9.2018 on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament

the signature of some Big Tech companies, an Action Plan against Disinformation was eventually released[123]. More specifically, the plan aims at involving the European External Action Service in setting up timely and effective responses to disinformation campaigns, encouraging the private actors that have agreed to the Code of practice to implement it and raising societal awareness about the risks associated with disinformation and manipulation techniques. More recently, even the EU Court of Auditors has published a report dedicated to disinformation[124].

Overall, there has been an enhanced focus and an increasing awareness in the EU framework about the challenges that disinformation and manipulation campaigns pose to democratic processes. Yet, the instruments adopted have proved ineffective to prevent their spread and the alteration of public debate, also in light of a preference for non-binding sources bearing a mere persuasive force towards the various stakeholders. As the binding EU sources already existing did not address directly this issue, due consideration will be given later to the analysis of the potential of the legislation proposed to redress some of these shortcomings (§6).

Reference to the system of the ECHR is also useful to build a comprehensive framework of the policies adopted to prevent an uncontrolled spread of disinformation campaigns all over Europe. While unable to rely upon binding instruments of legislation, the institutions of the Council of Europe have not ignored the saliency of this issue. The Venice Commission has first delivered a report on the impact of disinformation efforts on the fairness of electoral processes[125], while more recently an *ad hoc* set of principles for the use of technologies in electoral processes has been endorsed[126].

Actually, the issue of false statements in political communication was not entirely new to the Strasbourg court's case law, as the judges had already addressed the limits of alleged lies in politics in earlier decades, recognizing

[123] JOIN(2018) 36 final, Joint communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Action Plan against Disinformation.

[124] *Disinformation affecting the EU. Tackled but not tamed*, Special report No 09, 2021, European Court of Auditors, 15 September 2021, https://op.europa.eu/en/publication-detail/-/publication/392eeffe-1698-11ec-b4fe-01aa75ed71a1.

[125] K. Rozgonyi, *The impact of the information disorder (disinformation) on elections*, European Commission For Democracy Through Law (Venice Commission), CDL-LA(2018)002, 26 November 2018.

[126] *Principles for a fundamental rights-compliant use of digital technologies in electoral processes*, Opinion No 974/2019, CDL(2020)037, 11 December 2020, European Commission For Democracy Through Law (Venice Commission), 11-12 December 2020.

a fairly wide protection to personal opinions as opposed to objective facts[127]. It was only in 2019, however, that the ECtHR mentioned explicitly false information in adjudicating a case concerning the application of a criminal penalty for the alleged dissemination of fake news during an electoral campaign for a Polish local election. In *Brzeziński v. Poland*[128], the Court found that Art. 10(2) of the Convention does not allow much room for restrictions to free speech in case political communication or topics of general interest are concerned. Even acknowledging the necessity to fight against the dissemination of false allegations concerning candidates for political office to protect the integrity of the public debate, the ECtHR recalled that it is of paramount importance to ensure that all opinions and pieces of information are free to circulate. By considering the sanctions provided for by the Polish legislation incompliant with the principle of proportionality, the judges seem to have adopted a fairly tolerant approach with reference to lying in politics. Yet, a different stance has been put forth, which disregards the application of Art. 10 ECHR, in favour of the applicability of Art. 17. As the provision prevents the holder of a right to exercise it in ways that eventually harm the rights of other individuals, the standard of scrutiny on disinformation campaigns would be inherently higher[129].

The sample size is so far limited and does not take into account communication over social media platforms; nevertheless, the case law concerning offline political communication and the interpretation of the relevant ECHR parameters seem to suggest that the Court of Strasbourg would apply a fairly heightened scrutiny in assessing whether limitations to free speech aimed at containing the dissemination of fake news are proportionate and, in the end, legitimate exercise of the balancing power vested in State institutions[130].

The efforts undertaken within the EU context are proof that it is therefore essential to develop a concerted strategy to face the challenges posed both by, on one hand, the suppression of speech by digital intermediaries, the proliferation of unverified and alarming information

[127] *Lingens v. Austria* (Application no 9815/82) 8 July 1986, §46.
[128] 47542/07, 25 July 2019, I Sect.
[129] E. Shattock, *Should the ECtHR Invoke Article 17 for Disinformation Cases?*, *EJILTalk! Blog of the European Journal of International Law*, https://www.ejiltalk.org/should-the-ecthr-invoke-article-17-for-disinformation-cases/, March 26, 2021.
[130] A. Sardo, *Categories, Balancing, and Fake News: The Jurisprudence of the European Court of Human Rights*, in *Canadian Journal of Law & Jurisprudence* 2, vol. XXXIII, 435-460, 2020.

over social networking platforms and, on the other, the circulation of manipulative messages propelled by political actors seeking support from the voters. In the meantime, some States have come up with legislation laying down specific obligations for online intermediaries. To date, the most prominent example is the 2017 German *NetzDG*[131]; its scope of application, however, covers mainly content that would be anyway illicit offline, thereby imposing timely intervention by digital intermediaries upon the lodging of complaints alleging that content posted on a platform is unlawful. Yet, this example falls short of tackling specifically the issue of misinformation and manipulation of the news market, while being mostly concerned with the delimitation of the use of social networking platforms to perpetrate 'traditional' crimes[132].

Similarly, France has first imposed duties of transparency and reporting to digital intermediaries, while also establishing an ad hoc expedited judicial remedy for the removal of content that qualifies as misleading or inexact information and vesting the *Conseil supérieur de l'audiovisuel* with powers to refuse to grant dissemination privileges to foreign-owned broadcasters that spread false information[133]. The law has survived the scrutiny before the *Conseil Constitutionnel*[134] and it has entered into force just months after the *NetzDG*. Moreover, obligations to moderate specific illicit content (child pornography, terrorism, hate speech) were also introduced shortly after by the French lawmaker[135], along with duties to set up an internal complaint handling mechanism. Failure to comply by the platforms could trigger the imposition of severe monetary penalties or even imprisonment.

[131] *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken*, commonly known as *Netzwerkdurchsetzungsgesetz* (*NetzDG*), BGBl. I S. 3352, 1 September 2017.

[132] T. Wischmeyer, *What is illegal offline is also illegal online: the German Network Enforcement Act 2017*, in B. Petkova, T. Ojanen (eds.), *Fundamental Rights Protection Online*, Edward Elgar Publishing, Cheltenham, 2020.

[133] *Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information*, JORF n°0297 du 23 décembre 2018; see R. Craufurd Smith, *Fake news, French Law and democratic legitimacy: lessons for the United Kingdom?*, 11 *Journal of Media Law* 1, 52-81 (2019).

[134] Conseil Constitutionnel, Décision n° 2018-773 DC du 20 décembre 2018.

[135] *Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet*, JORF n°0156 du 25 juin 2020; see D. Steiger, *Protecting Democratic Elections Against Online Influence via "Fake News" and Hate Speech – The French Loi Avia and Loi No 2018–1202, the German Network Enforcement Act and the EU's Digital Services Act in Light of the Right to Freedom of Expression*, in S. Schiedermair, A. Schwarz, D. Steiger (eds.), *Theory and Practice of the European Convention on Human Rights*, Nomos Verlagsgesellschaft, Baden-Baden, 2022, 175.

Yet, the strict regime of the so-called *Loi Avia* was mitigated as some of its provisions did not pass constitutional muster and were thus struck down by the *Conseil Constitutionnel* before the law was eventually promulgated[136].

Even in those countries where criminal penalties were considered as viable remedies to tackle the spread of fake news, the actions taken have not necessarily been conclusive[137]. This discussion, indeed, does not address the 'elephant in the room', which is the exercise of ultimate authority by the owners of each platform over permissible content. However, vesting the digital operators with duties of removal of content that qualifies as illicit offline or in any case inaccurate does not settle all the underlying issues[138].

6. *The EU Digital Strategy between Intermediary Liability and Platforms' Accountability*

The spread and effects of phenomena such as political micro-targeting and disinformation campaigns makes it compelling to investigate if and to what extent digital intermediaries that operate the most widespread platforms should be regulated and encouraged to tolerate or censor speech by private political actors. In this regard, this paragraph will explore the potential and the shortcomings of the EU normative framework, by taking into account provisions already applicable and the proposals for regulations that are currently being discussed or have recently been approved.

The leaps made by the Internet over the last couple of decades have made the case for a revision of the EU normative framework. The single most relevant piece of applicable legislation was the E-commerce Directive[139], which encompasses a number of grounds under which IT providers are exempted from liability for the information transmitted, stored or made

[136] Conseil Constitutionnel, Décision n° 2020-801 DC du 18 juin 2020.

[137] R.K. Helm, H. Nasu, *Regulatory Responses to 'Fake News' and Freedom of Expression: Normative and Empirical Evaluation*, in *Human Rights Law Review* 2, vol. 21, 302–328, 2021, where the authors maintain that imposing criminal sanctions would be the best suited regulatory approach to fake news, rather than information correction or content removal.

[138] K. Kaesling, *Privatising Law Enforcement in Social Networks: Comparative Model Analysis*, in *Erasmus Law Review* 3, vol. 11, 151-164, 2018; L. DeNardis, A.M. Hackl, *Internet governance by social media platforms*, in *Telecommunications Policy* 9, vol. 39, 761-770 (2015).

[139] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

available. The only condition is that they do not play an active role in shaping its content and they act expeditiously to remove content due to its illegal nature or upon a judicial or administrative order[140]. The Directive adds a prohibition for Member States to implement any regime providing for a all-encompassing obligation of monitoring of content for providers of IT services.

The meaning and scope of application of some of these provisions has been clarified by the CJEU, which confirmed that blanket regimes of monitoring may not be imposed on social networking platforms, also to avoid excessive limitations to the enjoyment of the right to communication and passive information enshrined in Art. 11 CFR[141]. Moreover, the requirement of actual knowledge about the illegality of the content has been fully upheld by the Luxembourg Court, making irrelevant the mere notification of the existence of such content[142].

Against such a backdrop, the EU Commission has come up with three proposals of regulations aimed at distinct, yet connected, goals. On the one side, the Digital Markets Act (DMA) focuses on the obligations of so-called relevant gatekeepers to refrain from engaging in anti-competitive conducts by leveraging on the amount of users' data collected. On the other side, the Digital Services Act (DSA) is directed at complementing the liability exemptions of the E-commerce Directive with a series of obligations applicable to the operators of the digital market and layered according to the different nature of the activities at stake[143]. Lastly, the proposal for a regulation on the transparency and targeting of political advertising aims at laying down a harmonized framework for the safeguard of election integrity and the fairness of democratic debate. Consistently with the scope of the present article, the analysis will only touch upon the implications of the approval of the DSA and the prospective adoption of the draft proposal, in order to assess their impact upon the right of EU citizens to free speech, to information and to disseminate political messages.

First and foremost, EU institutions seem no longer satisfied to pursue the goal of harmonization of national legislations by approximation to common standards provided for in legislative instruments with weaker

[140] Arts. 12-15 E-commerce Directive.

[141] Case C-360/10, *Sabam v. Netlog*, §§ 48, 50.

[142] Case C-324/09, *L'Oréal v. E-Bay*,.

[143] R. Gellert, P. Wolters, *The revision of the European framework for the liability and responsibilities of hosting service providers. Towards a better limitation of the dissemination of illegal content*, Report for the Dutch Ministry of Economic Affairs and Climate Policy, available at <https://repository.ubn.ru.nl/bitstream/handle/2066/234104/234104.pdf>.

binding force, such as the E-commerce Directive. Rather, the Commission reckons it necessary to implement a directly applicable set of rules that require no normative implementation by domestic lawmakers, thereby enhancing the uniformity of the legal framework at EU level. The choice of a regulation is grounded in the potential negative effects arising out of diverging obligations imposed to intermediary platforms by national legislators in the past few years[144].

Building on this assumption, the DSA[145] acknowledges the relevance and breadth of the challenges posed by online advertisement on digital platforms, content customization mechanisms powered by algorithms and their impact on the public discourse[146]. Moreover, the act tries to design mechanisms and procedures that ensure effective and timely moderation by the platforms over illicit content upon orders issued by national authorities or notifications by users[147], while still preserving the liability exemption framework of the E-commerce Directive. In addition, self-regulation of intermediaries is encouraged through the drafting of codes of conduct[148]. As expected, the EU Commission's proposal has stirred a considerable number of comments and remarks, which have taken into consideration several of the topics addressed by the draft regulation[149].

The text does not depart dramatically from the provisions of the E-commerce Directive, whose liability exemptions are poured without major changes into the legislation under consideration, while paying due consideration to the interpretation by the CJEU. In this regard, a comparison with the legal framework in the USA may come at hand. §230(c) of the Communications Decency Act[150] provides for 'Good

[144] Recitals 2, 3 and 4 DSA.

[145] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), PE/30/2022/REV/1.

[146] Recital 63 DSA.

[147] Recital 34 DSA.

[148] Recitals 88 and 89 DSA.

[149] In addition to those already mentioned previously, see also A. Savin, *The EU Digital Services Act: Towards a More Responsible Internet* (February 16, 2021), Copenhagen Business School, CBS LAW Research Paper No 21-04, available at SSRN: <https://ssrn.com/abstract=3786792>; E. Chivot, *The new EU rulebook for online platforms: How to get it right, who will it impact and what else is needed?*, in *European View* 2, vol. 20, 121-130, 2021.

[150] Title V of the Telecommunications Act of 1996 (*An Act to promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid development of new telecommunications technologies*), Pub. L. 104-104, 110 Stat. 56.

Samaritan' protection for IT providers, thereby exempting intermediaries from any civil liability for actions carried out in good faith to restrict access to content that the provider itself or the users find objectionable on a number of grounds specifically exemplified. This provision, introduced to remedy a finding of the Supreme Court of the State of New York otherwise unfavourable to digital intermediaries[151], protects operators of platforms and providers of other telecommunications services both for active conducts and omissions[152].

Interestingly enough, the DSA does not go as far as encompassing a provision comparable to the 'Good Samaritan' rule. What is innovative is the incentive for hosting providers to investigate and remove content that is either illegal or incompatible with the terms of services of the platform, which does not imply a qualification of the intermediary's conduct as active, thereby preserving its eligibility for the liability exemptions (art. 6)[153]. In any case, the introduction of a binding mechanism of notice and take-down of illegal content marks a notable shift of the EU normative model towards a policy of regulation of the platforms, instead of a liability regime of the intermediaries[154]. More specifically, along with imposing information duties on the intermediaries with reference to orders of removal or to provide information (arts. 8 and 9), the DSA lays down distinct classes of due diligence and transparency obligations imposed to the different kind of operators of the digital market.

Generally, all IT intermediaries are bound to include in their terms of service detailed, easily accessible and clearly formulated information about their content moderation policies[155], while also being requested to publish once a year a report encompassing data relevant to assess the activity of content moderation carried out[156]. Moreover, hosting intermediaries shall implement mechanisms enabling any user to notify content allegedly

[151] *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995).

[152] C. Cox, *The Origins and Original Intent of Section 230 of the Communications Decency Act*, in *University of Richmond Journal of Law and Technology Blog* (Aug. 27th, 2020), https://jolt.richmond.edu/2020/08/27/the-origins-and-original-intent-of-section-230-of-the-communications-decency-act/.

[153] A. Kuczerawy, *The Good Samaritan that wasn't: voluntary monitoring under the (draft) Digital Services Act*, in *VerfBlog*, 2021/1/12, available at <https://verfassungsblog.de/good-samaritan-dsa/>.

[154] M. Buiten, *The Digital Services Act: From Intermediary Liability to Platform Regulation* (June 21, 2021), available at SSRN: <https://ssrn.com/abstract=3876328>.

[155] Art. 14 DSA.

[156] Art. 15 DSA.

incompliant with the terms of service of the platform or illegal under domestic or EU law; all notifications must be processed and specific feedback on each determination given, providing a sufficiently detailed statement of reasons as well for the decision to preserve the content or to take it down[157].

Online platforms, which disseminate content to the public, must set up a system of internal handling of complaints against the decisions to remove content or to suspend the access of a user to the account, while also guaranteeing access to extra-judicial means of dispute resolution[158]. Remedies against users that frequently post or share illicit content shall be put in place, as well as safeguards against the abuse of the notification mechanisms[159]. Transparency duties as to the nature of advertising content are provided for as well[160].

Eventually, very large online platforms (exceeding 45 million active monthly users within the EU) shall also carry out systemic risk analysis on a yearly basis, setting up proportionate and effective measures to mitigate these dangers. Moreover, they shall submit autonomously to independent audit to verify their compliance with the transparency and reporting duties and with the commitments undertaken by joining specific codes of conduct[161]. Furthermore, they shall set out clearly the main parameters driving recommendation systems that underlie the content shown to each specific user, allowing all subscribers to change in any given moment their own preferences in this regard[162]. The regulatory effort is supplemented by the encouragement addressed to digital market operators to draw up codes of conduct for the application of the DSA and for ensuring enhanced transparency in online advertising[163].

The text eventually provides for the implementation and enforcement of the above obligations through the establishment of a network of national Digital Services Coordinators, supported by a European Board for Digital Services[164], tasked with the duty to oversee the application and compliance with the regulation by hosting services and online platforms. A specific system of enhanced supervision managed by the EU Commission

[157] Arts. 16 and 17 DSA.
[158] Arts. 20 and 21 DSA.
[159] Art. 23 DSA.
[160] Art. 26 DSA.
[161] Arts. 34, 35 and 37 DSA.
[162] Art. 27 DSA.
[163] Arts. 45, 46 and 47 DSA.
[164] Arts. 49 and 61 DSA.

would be vested with the oversight over the conduct of very large online platforms. Noncompliance with the obligations laid down in the regulation, with interim measures adopted by EU Commission's decisions or with commitments undertaken by the platforms themselves would be subjected to monetary penalties calculated in percentage of yearly or daily revenues[165].

In November 2021, the European Commission has approved a draft proposal for a regulation on the transparency of political advertising techniques, including that of online targeting, which is currently under discussion in both national Parliaments and EU co-legislators. Its main goal is to provide for a harmonized legal framework and for a high level of transparency in political advertising within the EU. Adjunctively, it aims at complementing the already existing framework of personal data protection by envisioning rules – that would apply to all data controllers, not only to political advertising firms – on targeting and amplification techniques in political advertising. To the purposes of this discussion, it is interesting to analyse if and the extent through which the Commission's proposal may impact the right to freedom of expression. Firstly, by trying to provide for a harmonized understanding of 'political advertising', the draft proposal outlines an overly broad definition[166], which could be in tension with the right of freedom of expression, also in its passive nuance of right to receive clear and impartial information. Indeed, any form of speech – also legitimate criticism over current political systems, physiological in a democratic pluralistic society – could virtually fall under the scope of "a message […] which is liable to influence the outcome of an election or referendum, a legislative or regulatory process or voting behaviour", thereby being subject to the rules provided for in the draft proposal. Moreover, the scope of this proposal would be wider than the DSA's, that the draft is meant to complement. Indeed, while the latter exclusively addresses intermediary services, such as for example social media and marketplaces, the former encompasses both legal and natural persons. To the scope of the proposal, a 'political advertising publisher' would be any subject who broadcasts, makes available through an interface or brings to the public domain political advertising through any medium (newspapers,

[165] Arts. 74 and 76 DSA.

[166] According to Article 2(2) of the proposal: «'political advertising' means the preparation, placement, promotion, publication or dissemination, by any means, of a message: (a) by, for or on behalf of a political actor, unless it is of a purely private or a purely commercial nature; or (b) which is liable to influence the outcome of an election or referendum, a legislative or regulatory process or voting behaviour».

television, radio, social media and computer games). Therefore, any of these actors would be under the transparency requirements provided, which implies administrative burdens and higher costs, that could affect the freedom of expression and the right to receive information, without any form of journalistic exception.

In light of the prospective framework outlined above, some considerations will be offered in the final paragraph as to the desirability of the EU approach to content moderation, intermediary liability and transparency in online political advertising, by drawing inspiration also from comparative examples and taking into account the risks underlying the role of online platforms in shaping the public discourse and influencing the outcome of electoral contests.

7. *Regulatory Frameworks at Supranational and Domestic Level: Freedom of Speech and Information between Constitution, Legislation and Self-Regulation*

Given the practical relevance of the phenomena of political micro-targeting and fake news in the context of online debate and their potential to alter the proper functioning of the public sphere, three possible approaches appear available to European lawmakers to effectively tackle disinformation and manipulation of political discussion online. Understanding where the DSA and the Draft regulation on online political advertisement stand against this threefold alternative makes it possible to assess whether the policy and legislative choices adopted fit the EU constitutional framework as described earlier.

First, legislators could withhold completely from the informational market and request the platforms to limit their intervention over content that is posted, removing only the posts that manifestly qualify as illicit according to ordinary law. Moreover, such an approach would apparently be the most favourable to the freedom of speech of users and would also lift an otherwise relevant burden from the shoulders of the platforms. The latter, in fact, would be exempted from exercising but a limited activity of content moderation, not being subject to meaningful incentives to remove content unless upon judicial request. This approach would likely minimize the risks associated with collateral censorship[167]. In fact, the digital

[167] The concept of collateral censorship was first outlined by M.I. Meyerson, *Authors,*

intermediaries would enjoy almost no leeway in determining whether a content deserves to appear on the platforms or deserves removal. Also, following this model would imply embracing a fairly hard-line version of the theory of horizontal effect of constitutional provisions, which would bind digital platforms as much as public bodies.

In this context, users could claim the infringement of their freedom of speech against the platforms in case their content was allegedly removed or moderated illegitimately (*i.e.*, outside the legal rules applicable also to offline conducts). Also, political actors would enjoy a wider discretion in shaping the content of their political messages, therefore making it more likely that disinformation, be it generalized or micro-targeted towards specific voters or niches of electors, spreads all over these platforms. This one option would expand the breadth of the cleavage between EU and US regimes of freedom of speech, as private intermediaries would be compelled to host speech that they would otherwise not tolerate or disseminate[168].

Second, there could be an intermediate approach centred around the regulatory functions of States or international organizations with binding normative powers, enhancing the role of lawmakers in framing the instances when social networking platforms are required to remove or moderate content under the threat of monetary penalties. In this case, there would be no (in)direct effect of constitutional provisions over private legal relationships, but a mediation in the guise of explicit State legislation would be needed to balance the freedom of speech of individuals and the interest in the authenticity of online debate.

The legislative efforts undertaken in Germany and France in recent years appear to have followed this avenue, as they have introduced regulatory frameworks specifically designed to apply to digital intermediaries. Yet, both seem to have made extensive use of reference techniques in the legal drafting, by recalling criminal provisions that apply also offline, to identify conducts that must be sanctioned when taking place onto online platforms as well. Within this logic of reconfiguration[169], this new set of rules brings

Editors, and Uncommon Carriers: Identifying the Speaker within the New Media, in *Notre Dame L. Rev.* 1, vol. 71, 79-125, 1995; the issue has been then explored more in detail in the following years, starting with J.M. Balkin, *Free Speech and Hostile Environments*, in 99 *Colum. L. Rev.* 8, 2295-2320 (1999), 2298.

[168] Envisaging a symmetrical application of offline legislation to online speech forecasts a series of prospective problems, see Chris Reed, *Online and Offline Equivalence: Aspiration and Achievement*, 18 *International Journal of Law and Information Technology* 3, 248–273 (2010).

[169] T. Wischmeyer, *Making social media an instrument of democracy*, 25 *European Law*

about an element of novelty only for what concerns their subjective scope of application (*e.g.*, hosting and social networking platforms) and the procedural guarantees that the market operators must comply with; however, there appears to be no revolutionary approach for what concerns the factual conducts that are targeted, which mostly resemble activities that were illegal also offline.

Third, public powers could reckon it wiser to leave it to the informational market to determine how to control the content uploaded, by relying on the various models of terms of service valid for each platform. The preference for self-regulation would approximate the European attitude to the US context, even if in the latter framework this result is directly connected to the extension of the prerogatives granted under the Free Speech Clause to private legal entities[170]. Yet, this option is the one which makes it more and more likely the risk of surrendering censorship functions to digital intermediaries, whose role of gatekeepers would imply a careful assessment of the dynamics underlying the phenomenon of collateral censorship already denounced earlier[171].

Against this threefold alternative, due consideration must be given to what was already pointed out earlier on, when dealing with the size – both in terms of revenues and of subscriptions – of digital intermediaries and the fact that their operations are transnational in nature[172]. This implies that efforts undertaken single-handedly by States appear increasingly inadequate to prevent the drowning of the public opinion towards a situation labelled by some as an *infodemic*[173]. To make up for the deficiencies inherent to State legislative regimes, resort shall be had to sources of international law or that, in any case, have a wider territorial scope of application, such as those of the European Union.

Journal 2, 169–181 (2019).

[170] R. Tushnet, *Power without Responsibility: Intermediaries and the First Amendment*, 76 *Geo. Wash. L. Rev.* 4, 986-1016 (2008).

[171] J. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, in *U.C.D. L. Rev.* 3, vol. 5, 1149-1210, 2018, 1174.

[172] A. Mills, *The law applicable to cross-border defamation on social media: whose law governs free speech in 'Facebookistan'?*, in *Journal of Media Law* 1, vol. 7, 1-35, 2015; O. Bigos, *Jurisdiction over cross-border wrongs on the internet*, in *International & Comparative Law Quarterly* 3, vol. 54, 585-620, 2005.

[173] The term was coined by the American journalist David J. Rothkopf about the information epidemic concerning the spread of the SARS virus in 2002 (*When the Buzz Bites Back*, *Washington Post*, 11 May 2003); reference to it has been made by the WHO and the EU Commission more recently concerning information circulated during the Covid-19 pandemic.

The actions encompassed within the EU's approach to tackling challenges in the digital framework stem from the General Data Protection Regulation (GDPR), the EC-initiated code of self-regulation of platforms (Code of Practice on Disinformation), and the non-binding Commission's communications and recommendations to the Member States. Moreover, some new measures are provided for in the AI Draft for Regulation, in the DSA and DMA and in the European Commission Draft on Greater transparency in paid political advertising. While some of the measures have reached a high level of accuracy and have been constantly developing, some approaches represent new steps in trying to regulate digital phenomena. The European approach towards the analysed phenomena is currently designed towards the prevention of unlawful micro-targeting and the battle towards disinformation by increasing the transparency of political ads on digital platforms.

Assessing the prospective policy choices that seem likely to come into force in the EU legal framework, it is possible to provide essential remarks as to the normative strategy that European institutions appear to have followed. Notably, both the DSA and the proposal for transparency in political advertising may be ascribed to the second regulatory approach set forth above. As a matter of fact, the legislation that is being considered introduces a set of procedural obligations applicable to digital intermediaries and, to a limited extent, to all the actors involved in political communication. The above considerations show that only a concerted effort by EU and Member State institutions, digital intermediaries, and citizens is capable of maximising the chances to build effective barriers against phenomena such as political micro-targeting and disinformation campaigns, that threaten the stability and well-functioning of modern pluralistic democracies built on a deliberative model. Only time will tell if these anti-bodies last long enough to prevent a deadly disease for this paradigm.

Fabiana Di Porto, Marialuisa Zuppetta

Co-regulating algorithm disclosure for digital platforms

Abstract: With digital platforms gaining dominant intermediating role and exerting regulatory functions vis-à-vis small and medium-sized enterprises (SMEs) through algorithms, EU institutions have started considering to rely on their analytical capacity to regulate the myriads of market transactions occurring within and through them (so-called platform-to-business, or P2B transactions). Most of the time, the EU suggests recurring to light-tough disclosure duties. Hence, the European model falls short in rebalancing information asymmetry and unequal bargaining power plaguing the SMEs. In practice, the EU model consists either in pure delegation of self-regulatory powers (codes of conduct) or nonenforceable co-regulatory schemes (with technical standards established by the platforms themselves). Other models have been suggested that rely on the regulator's access to the platform's data (so called savvy and data-delegated options). These governance models present several limitations, making the platforms' role as regulatory intermediators little credible. In this scenario, the paper purports that a third option should be considered. In particular, to tackle the multifaceted risks associated with algorithmic decisions by digital platforms, while at the same time avoiding stifling innovation, it makes three suggestions: (1) also information disclosures should be done by an algorithm; (2) that is pre-tested in a co-regulatory process, that involves the regulator and stakeholders; and (3) enforced through legal and other empowerment tools, rather than sole fines.

---

* This article was first published in *Policy and Society*, vol. 40, N. 2, 2021, pp. 272-293. Previous versions of this paper have been presented at the Workshop on 'Data Economy', organized by the Body for European Regulators for Electronic Communications (Berec) in Brussels on May 14th, 2018, at the Annual Conference of the Italian Society of Law and Economics (ISLE), held in Lecce on December 14th, 2018 and at the attendants to the 'EU Regulation of Digital Platforms' seminars held at the Law Faculty of the Hebrew University in November- December 2019; the 15th Annual conference of the Academic Society for Competition Law (Ascola), 25-27.6.2020 (available here: <http://youtu.be/VO9FcZxLVP4>). *Original dedication*: We are thankful to the discussants and the anonymous referees for their very useful comments. All mistakes remain ours. The article has been jointly conceived; however, Marialuisa Zuppetta drafted the Introduction and sect. 2; while Fabiana Di Porto the other sections. This article is dedicated to the beloved memory of co-author Marialuisa, who passed away too early.

1. *Introduction*

Since the past decades, digital platforms (defined à la Evans & Schmalensee, 2016)[1]1 have become essential intermediaries in the daily lives of individual consumers and the small business (SMEs) alike. These technologies have been enhancing their capabilities to interact, organize, move, buy, purchase. That has been possible thanks to the broadest sharing of data and information among all market participants and their intermediation through powerful Information Technologies (IT). Yet, for long the need to let digital innovation develop made public intervention undesirable to most regulatory institutions at the European level (EC, 2016a Feb. 2nd) and the U.S. ones (FTC, 2016; Exec. Order No. 13,859, 2019[2]; Office of Science and Technology Policy, 2020; contra: Stigler Group, 2019, calling for regulatory intervention, eg. to react against 'dark patterns')[3].

More recently, however, calls for regulation of digital platforms have gained momentum among theoreticians, as well as EU institutions. As platforms in many areas have become 'superdominant' or quasi-monopolist and engaging in anticompetitive conduct against their small-business counterparts, competition scholars have started questioning whether antitrust policy 'should take a tough stance' against digital 'ecosystems' that auto-reinforce their positions in their well-protected 'walled gardens' (EC, 2019, p. 16; Evans & Schmalensee, 404; Tirole, 2017; OECD, 2018; Stigler Group, 2019).

For instance, big digital platforms can exploit their informative advantage to self preference their products against their small business rivals'; or degradate the prominence of their competitors' offers by simply manipulating the algorithms managing rankings, or they may terminate

[1] We are not dealing with all platforms, but only with 'matchmakers', intended à la Evans and Schmalensee (2015): i.e. those connecting suppliers and consumers through algorithms, and reducing search costs for both. This would essentially exclude from the analysis: blogs and platforms such as Facebook, Google's AdSense, Amazon Web Services or PaaS and include e-commerce, price comparison sites and search engines.

[2] Exec. Order No. 13,859, *Maintaining American Leadership in Artificial Intelligence*, 84 Fed. Reg. 3967, 11.2.2019

[3] Note that exceptions to this light-handed approach have always existed: examples of ex ante regulation are the 'Access to account data rule' in the Fintech sector (Di Porto & Ghidini, 2020); the mandated exchange of electricity and gas smart metering information (Directives 2019/944/EC and 2009/73/EC); the access to electricity network data rule (Commission Regulation (EU) 2017/1485), and, of course, intelligent transport systems (Directive 2010/40/EU).

traders' service contracts without stating any justifications[4]. Moreover, the need to proactively further an EU-wide Digital Single Market (EC, 2015) into a broader European Data Economy, (EC, 2017, 2018) recommend initiatives aimed to tackle the limited bargaining power and lack of information of business users (EC 2020c; operating in and through platforms[5]. This tougher stance is now reflected in the debate surrounding the Digital Services Act Package 2020 (EC, 2020a, 2020b), where the Commission is considering ex-ante rules as part of a pro-competition reform debate (EC, 2020d)[6]. If implemented, new measures will be adopted to expand existing transparency duties; and increase the number of data sharing agreements being stipulated between the big platforms and their SMEs counterparts. As a default, such agreements will be voluntary; but ex ante access to platforms' data might be mandated if sector-specific market failures are detected that standard competition rules cannot solve (EC, 2020a, at 3–4; 2020d.)

In parallel, thanks to thicker knowledge on the possible harm to SME users (and the society more broadly) deriving from decisions led by algorithms and Artificial Intelligence (or AI), (Taeihagh, 2020), a need for protecting the small business beyond the rights entrusted by existing EU legislation, has also been raising (EC, 2020c). Data market power is pernicious because it provides large platforms with wide regulatory powers that go undetected to traditional oversight. For instance, big digital players may 'set the rules on the platform and unilaterally impose conditions for access and use of data' over their SMEs counterparts (EC 2020a, p. 8).

Hence, the academic quests for explicability, transparency and accountability of AIled decisions (eg. Ananny & Crawford, 2016; Heemsbergen, 2016; Stohl, Stohl, & Leonardi, 2016), have turned into a policy imperative (Council of Europe, 2019; European Parliament - EP,

[4] Executive summary of the Impact Assessment (SWD (2018) 139 final) accompanying the Proposal for Regulation Regulation 2019/1150, at 2.

[5] See EU Regulation 2019/1150 of the European Parliament and the Council on 'Promoting fairness and transparency for business users of online intermediation services', of 20.6.2019, OJEU L-186 of 11.7.2019.

[6] The debate recalls the standard literature on the need to regulating monopolies, whatever the sector: any market player enjoying extensive market power has the potential to exploit it at the detriment of its competitors and clients. Because antitrust rules might not be sufficient for tackling these behaviors, quasi-monopolists are often regulated. Stated otherwise, monopoly or quasi-monopolies are rationales justifying regulation. What is peculiar of digital platforms that enjoy market power (think e.g. to Google search engine in the EU Google case), is the algorithmic means by which they exercise it, as discussed thoroughly in the text. For further details, EC (2019).

2019b; EU High level Expert Group on AI, 2019; OECD, 2019). For instance, the Council of Europe has urged Member States to take measures against illegitimate forms of interference by AI tools[7]. 'exploit their data' to. It suggests empowering users by robustly enhancing awareness of how platforms 'exploit their data' to train algorithms for commercial purposes[8].

The European Parliament (EP 2019b) makes a step forward. Like the Council of Europe,, it warns on the ability of algorithms to violate expectations the SMEs fiduciary expectations the SMEs have toward organisations using the same AI systems; on the other[9], to contain this, it calls for empowerment strategies that are based on AI tools: '[I]n the AI era, an effective countervailing power needs to be supported by AI too'[10]. Interestingly, the EP considers AI-led empowerment tools more effective than traditional public regulation and enforcement to reduce AI-led manipulation (such as price discrimination, and over-targeting), suggesting that data mining algorithms could be used in manyfold ways to help SMEs, from 'analysing and summarising massive amounts of reviews, or comparing prices accross platforms,' to 'detecting discrimination' or 'build [ing] supporting tools that could identify prejudice an unfair treatments'[11].

* * *

Clearly, the need for regulatory intervention is being gradually established (*why*), as is its addressee (*whom*) – the big digital platforms – and the beneficiaries – the SMEs. The latter are emerging as subjects in need of protection vis-à-vis their platforms' counterparts on several grounds:

1 they suffer from information asymmetry and

2 low bargaining power because they cannot but operate their business through the platforms, who, in turn, manage these massive markets through

3 regulatory powers, which they exercise

[7] Council of Europe (2019): 'Contemporary machine learning tools have the growing capacity not only to predict choices but also to influence emotions and thoughts and alter an anticipated course of action, sometimes subliminally' (pt. 8). Digital technologies can 'use personal and non-personal data to sort and micro-target people, to identify individual vulnerabilities and exploit accurate predictive knowledge, and to reconfigure social environments in order to meet specific goals and vested interests' (pt. 9).

[8] Ibid., pt. 9, lit. e).

[9] EP, 2019, at 5.

[10] Ibid., at 7.

[11] Ibid, p. 8.

4 via algorithmic decisions fed by big data[12].

And because black box-based, such algorithmic decisions, add a layer of opacity to the platform-to-business (or P2B) relationship, thus worsening the information asymmetry and low bargaining problems of SMEs (1 and 2).

If the why for regulating and *whom* are more or less clear, there is still little agreement as far as the regulatory governance model to put in place the resulting and the tool/s to employ (*how*). On the one hand, to tackle information asymmetries and resulting low bargaining power plaguing SMEs, the EU institutions propose using traditional disclosure regulation (panacea) to increase transparency and accountability of platforms' business algorithmic decisions. Others contend that because platforms perform a 'visible hand' function (by providing rankings and ratings, match-making and an information intermediation function) traditional disclosure regulation should be dismissed altogether and pure algorithmic self-regulation by the platforms (Ben-Shahar & Schneider, 2011, 2014) .

We contend that disclosure regulation could indeed still play a role to empower platforms' business users, but to do so it should be rethought of. Following the EP's suggestions, European institutions should consider designing disclosures through algorithms, and also privilege the involvement of platforms, which enjoy regulatory functions, as credible actors in a data-based co-regulatory governance structure.

This article fills a void in the literature. While a lot has been said about individual consumers' inability to cope with algorithmic decisions affecting their autonomy in online marketplaces, (Gal, 2017; Susser, Roessler, Nissenbaum, 2019; Zuboff 2019) the same does not hold for micro and small-sized enterprises (SMEs). Regarding the latter, the literature mainly focuses on competition analysis, (Evans & Schmalensee, 2015) or the contractual profiles of P2B relationships, (de Streel & Sibony, 2017) while does barely indulge on how to devise disclosures that can work for them, in a digital environment. This contribution links the literature on regulatory intermediation (Abbot, Levi-Faur, & Snidal, 2017) with the legal doctrine on disclosure duties in P2B relations to reach a proposal for the legitimate use of algorithms to produce disclosures in a participated governance.

The article is, therefore, organized as follows. We start by collocating digital platforms in the realm of regulatory intermediators, by scketching how their regulatory functions differ from traditional ones, being them

[12] To make an example, Coglianese and Lehr (2019), at 9 see the 'fully automated dispute resolution system developed and already used by eBay to settle tens of millions of disputes each year' as a form of 'adjudication by algorithms'.

excercised through powerful algorithms trained on massive data collected (also) from the SMEs. Algorithmic regulatory functions of digital platforms are thus classified and analyzed to spot their impact on the life of SMEs operating in and through them. Several criticalities are found that are only marginally tackled by the EU. For this reason, sections 3 and 4 present the two regulatory governance models through which the EU has reacted to the severe information asymmetry and subsequent unequal bargaining power of the SMEs. These are: Disclosure self-regulation enacted through Codes of Conduct (sect. 3); and Disclosure Co-Regulation enacted through light cooperation with digital platforms (sect. 4). As we shall see in sect. 5, both models suffer severe limitations, making big platforms's role as regulatory intermediators little credible. That leads us to discuss new models, where the circulation of data between the platform and the regulator is at the core of intermediation. That provides the theoretical framework for our proposal (sect. 6), where AI tools are used to generate algorithmic disclosures in a participated and experimented fashion. Sect. 7 discusses our model and concludes.

2. *Regulatory functions of digital platforms. Classifications and issues*

Already in 1999, Lessig (1999) recognized that technology could complement or even be a substitute for legal regulation ('code is law'). Scholars from the social sciences have theorized that not only the technology but any actor, private or public, (such as NGOs, certification bodies like Data Protection Officers (Medzini, 2018), or the US Security Council) can play 'major and varied roles in regulation', serving as 'regulatory intermediators' (Abbot, Levi-Faur, & Snidal, 2017)[13]. In their view, intermediators add a layer to the dual relationship between the regulator and its targets, by acting 'in conjunction with a regulator to affect the behavior of a target'[14].

It comes as no surprise that Cohen and Sundararajan (2015) have extended the concept of regulatory intermediators to digital platforms; after all, they had been conceptualized as 'infomediaries' since the

[13] Abbot et al. (2017) (contending that regulatory intermediators may give support by 'providing expertise and feedback to facilitating implementation, from monitoring the behavior of regulatory targets to building communities of assurance and trust.', at 19). See also the Special issue of Reg.&Gov (2019).

[14] Abbot et al, previous note, at 19.

Nineties (Gaudeul & Jullien, 2008; Hagel & Rayport, 1997) and later on as 'matchmakers' by Evans & Schmalensee). According to them, in the growing world of peer-to-peer, digital platforms can be accounted as credible parties in the regulatory arena, because they enjoy regulatory functions. Indeed, when designing its own architecture, a platform defines the rules governing the space where users operate; and in doing so it proceeds from a 'macro-level' down to a 'micro-level', where interactions between platforms and business and among peers are regulated at a very detailed level[15]. That is done through algorithms fed by data produced within the platform[16]. It follows that the kind of regulation produced at the 'micro-level' is not only algorithmic[17], but also highly 'granular', compared to traditional (i.e. nonalgorithmic) legal rules[18].

For what interests us, the regulatory functions of platforms can easily be grouped into three main functions: (i) setting the architecture design; establishing rules governing (ii) the P2B relationships; and (iii) the interactions between users. Examples of (i) may be: the very design of an algorithm (as is the case with search engines, providing ranking of search results)[19], or the design of rules and institutions that 'shape the functioning of the marketplace' (EC, 2019 at 60). As per (ii), platforms are the ones

[15] Rules produced in these environments tend to have a 'higher degree of granularity without prohibitively high complexity costs': Busch (2019), at 12.

[16] EC (2019), at 60.

[17] Speaking of algorithmic regulation might sound a tautology, given that algorithms are themselves rules. However, one thing is to define rules for using the platform based on free negotiations between SMEs and the said platform. Other thing is that such rules are drafted by the platform using an algorithm that derives the knowledge of the SME's preference from the data it gathers by the SME's usage of the platform. In this case, the information asymmetry is essential, as is the bargaining power of the two counter-parts.

[18] Black (1996), at 27 speaks of 'individualised regulation' to refer to regulation tailored at the single, individual firm. More recently, see: Strahilevitz and Porat (2014); Busch (2016b); and Busch and De Franceschi (2018).

[19] Algorithmic decision-making may also re-ontologize the world 'by understanding and conceptualizing it in new, unexpected ways, and triggering and motivating actions based on the insights it generates'. 'The most concrete example is the ways in which artificial agents construct the available action space of online environments, such as search engines that make available links to other websites through an algorithmic ranking. Algorithms are, in this regard, part of a process of "reality construction" by including or omitting specific information that, in effect, governs behavior and actions. 'The fact that artificial agents, through the computational generation of knowledge, can constrain, alter and nudge behavior towards a specific goal has also been conceptualized as "algorithmic regulation", "governance by algorithms", of algorithms as "artefacts of governance", and "algorithmic governmentality"' (Gahnberg, 2020, p. 5-6).

regulating the way data generated therein may circulate (e.g. limiting it to the use of application programming interfaces, or APIs); may impose price controls or fix the rating and recommendation policies. Concerning user-to-user relations (iii), it is the platform that typically establishes standard models for presenting commercial offers; decides about delivery and returning policies, and so forth. (EC 2019, at 61).

While algorithmic production of rules by the platforms can be cost-effective, as it 'suits the scale of peer-to-peer' (EP, 2017 at 23) (flexibility and differentiability), and may generate efficiencies, by allowing transactions that were not possible before such innovations, there are nonetheless issues that need to be tackled.

First, business users cannot know what the parameters used in algorithmic decisions are, nor can they be sufficiently aware of the legal consequences of the decisions taken by the platforms. Often, the data produced through the use of the platform – which is machine-generated data – tend to be treated as belonging to it, and therefore not accessible to the business user. Think for instance to marketing data in marketplace platforms like Amazon: while these data are generated thanks to its users' interaction, they are nonetheless unavailable to them[20]. That puts the latter in a disadvantaged position vis-à-vis the platform, because they may not reuse it to profile their products or service further, and thus ameliorate them.

Moreover, some biases are 'innate' to the use of algorithms and that depends on the datasets, such as overreliance on correlations, which might generate discrimination among users or disadvantaged treatment (think, e.g. to ranking manipulation) (Lim & Taeihagh, 2019).

Furthermore, many business users are still uninformed of the real profit-driven mechanisms governing digital platforms (Whittington & Hoofnagle, 2012, at 1357; Acquisti & Grossklags et al., 2007). Often, digital platforms may take advantage of their users, who cannot understand and benefit from the full value of the data they generate, nor can they understand entirely the rankings practices applied to them. The myriads of micro and SMEs, as we shall see[21], are not the big business and often behave much like individuals, who have no share in the vast amounts of profit that platforms make out of the personal data they circulate (Grunes,

[20] Clearly, unlike those we are dealing with in this article, there are platforms that are likely to be aware of some main parameters, and for which sharing business analytics is a part of the value proposition from the platform (think e.g. of Google Analytics for designing one's own website). Moreover, for platforms of this kind, data sharing is an intrinsic part of the service (think e.g. of a marketing platform).

[21] See sect. 6, below.

2013, at 1123; Shelanski, 2013; Argenton & Prüfer, 2012; Vaidhyanathan, 2011; Rust, Kannan, & Peng, 2002).

In the same vein, with online bargains, SMEs' room for negotiation has shirked down, as is their bargaining power; digital platforms enjoy a strong information asymmetry against business users, which they can use to profile them and, accordingly, put themselves in the position to exploit and discriminate among and against them[22].

The European response to those problems, thus far, has been far from the interventionist, and has relied heavily on traditional informational duties. Although there might be some change in the future[23], the kind of legislative initiatives the EU has adopted range between delegation of pure self-regulatory powers to the platforms (in the form of codes of conduct), to co-regulation via the setting of EU principles coupled with technical standards established by the platforms themselves. Notwithstanding these differences in the governance structure, however, the kind of disclosure regulation adopted is quite standard (i.e. non-targeted, non-differentiated, and general): it merely suggests employing transparency duties regarding contract terms and conditions, and to release information about data use, or reputation mechanisms. In no way does it encompass or avail of algorithmic tools, as purported by the EP to better empower platform's business users, and their participation to the making of platforms' decisions (e.g. their codes of conduct) is only marginal.

In the following, we will review and discuss the EU model, starting with disclosure self-regulation (sect. 3). Here, recent legal initiatives encouraging platforms to design codes of conduct (or CoC) in the domains of personal data protection and non-personal data circulation will be analyzed.

3. *The European model: relying on (traditional) disclosure platforms' selfregulation*

Despite the many criticism disclosure regulation has undergone in the last decade (Ben-Shahar & Schneider, 2011, 2014; Craswell, 2006; Easterbrook & Fischer, 1984; Marotta-Wrugler, 2014; Prat, 2005)[24] it is

[22] EC (2019), at 62.

[23] We refer to EC, 2020a, 2020b and 2020d.

[24] Markets are flooded with too much information, and because many of its drawbacks are irresolvable, disclosure regulation should be dismissed altogether. The advent of the sharing economy could determine the end of information asymmetries without any piece

still the preferred mode of intervention by the EU institutions vis-à-vis big digital platforms. The European Model accounts for dozens of novel informational duties that have been introduced despite little evidence of their effectiveness[25].

3.1. *(Traditional) Solicited Codes of Conduct: the GDPR and EU regulation 2018/1807*

Self-regulation by digital platforms is at the core of EU initiatives aimed at the liberalization of non-personal data circulation (Regulation UE 2018/1807)[26]. Platforms are 'encouraged' to adopt self-regulatory CoC to provide (also) professional users with 'detailed information and operational requirements for data porting' and the switching of the service provider[27]. The porting of data from one provider to another being fundamental to create the broadest and most competitive data economy, EU institutions consider it essential that professional users are 'aware' of such possibility. Therefore, the CoC should, first of all, establish communication roadmaps to 'raise awareness' about the CoCs themselves (Art. 6(d)). They should furthermore include 'sufficiently detailed, clear and transparent [technical] information regarding' the switching, that professional users should receive 'before a contract for data processing is concluded' (Art. 6(b)).

Similarly, concerning personal data, the EU GDPR No. 2016/679, foresees several disclosure obligations (Arts. 40 and 41), whereby platforms or their associations (as data controllers and processors) are encouraged to

of disclosure regulation, provided that peers exchange their opinions by writing reviews and relying on a network of feedbacks and ratings.

[25] Contra Busch (2016a), 223, (discussing the weaknesses of platforms' reputation systems and suggesting safeguarding measures to fix them). See also Finck (2017), at 14 (contending that although platforms have access to myriads of data that regulators do not possess, which could help to draft proper disclosures, they nonetheless lack the public interest view required to decide what piece of information, at what time, to whom and why should be disclosed).

[26] See Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. In OJ L 303, 28.11.2018, p. 59–68.

[27] Recital 30, Reg. EU 2018/1807. The codes of conduct should define Guidelines at the EU level on best practices that might 'facilitat[e] the switching of service providers and the porting of data' (Art. 6(a)).

lay down CoCs to 'demonstrate compliance with the Regulation'[28].29 In particular, platforms should provide information (amongst others) about the automatic treatment of personal data, including their collection, pseudonymisation, and processing. They should also provide information about the exercise of the rights of data subjects; and to self-assess the risks of data breaches (Article 40(1), lits. a-f), h), i)).

In its 2019 Guidelines on Codes of Conduct, the EDPS[29] distinguishes between an industry and nation-wide CoC and a transnational pan-European one[30]. Only the latter would have certifying effects within the whole EU (and to some extent even outside Europe), and thus entail some minimal regulatory powers to the EU Commission[31] (alongside with the National Supervisory Authorities grouped in the EDPS' council). It should be acknowledged, however, that the procedure to have a pan-European CoC approved is overly complicated and demanding[32].

In the former case – of national CoC – codes containing disclosures

[28] See Recital 13, GDPR. See also EDPS, (2019).

[29] EDPS, (prev. fn)

[30] I.e. a code entailing processing activities in more than one Member State: See Annex 1 to EDPS (2019).

[31] Ibid, pt. 59: 'The Commission may decide by way of an implementing Act that an approved transnational code will have general validity within the Union and shall ensure appropriate publicity if they were to do so.' See Articles 40(9) and 40 (10) GDPR.

[32] In a nutshell: a body representing categories of controllers or processors, including micro and SMEs, drafts a CoC which identifies a list of competent Supervisory Authorities (SAs) among EU ones. It indicates the criteria justifying which one, among those, be selected as Supervisory Authority (CompSA), serving as a one-stop-shop authority. It then submits a transnational CoC defining substantial rules and a monitoring body for ensuring compliance. A successful CoC application should demonstrate that: most extensive consultations were carried out before drafting; the draft code is compliant with Member State law(s); the monitoring body meets the independence and accreditation criteria (following Art. 41, GDPR). The CompSA will then notify the CoC to all SAs in search of one or two possible co-reviewers for receiving assistance in the CoC assessment. Within a 'reasonable period of time' (Guidelines, pt 52) the CompSA will submit the CoC to the EDPS' Board for approval (Art. 40(7) GDPR). Here, a further negotiation phase starts, with the Board being allowed to make comments (Art. 64 GDPR) and eventually rejecting approval. Once approved by the Board, the CompSA may still disagree with its Opinion, and therefore with the proposed CoC draft (Art. 40(5) GDPR), or it may finally approve it. Together with the approval of the international CoC, comes (as a conditio sine qua non) the accreditation of the monitoring body. The latter works closely with the CompSA (e.g. for complaints handling, monitoring compliance by adopting remedial actions ranging from warnings to the formal exclusion) and its decisions are made publicly available. A CompSA may revoke accreditation if the monitoring body fails to comply with its duties (Art. 41(5) GDPR).

would still be adopted by platforms voluntarily[33] as would the establishment of a monitoring body.

3.2. *Critical assessment of (traditional) disclosure self-regulation (codes of conduct)*

Among the many forms it can take (Black, 1996, 2001), here, disclosure self-regulation would be 'solicited' (i.e. not mandated) by public authorities (the EU), instead of adopted on a purely voluntary basis. That is because platforms are only 'encouraged' to enact CoC, and no reaction is foreseen in case they fail to do so. One could contend that the industry has a 'reputational incentive' to adhere to a CoC (besides the economic one[34]), especially when sensitive questions like the treatment of digital data are at issue.

However, as purported by Graef, Gellert, & Husovec (2018), incentives to draw a CoC can sometimes be misaligned to those of the regulator to the point that they can collide with the public goal pursued. That happens, in their view, with Regulation 2018/1807[35], where an EU-wide CoC disciplining the sharing of non-personal data stemming from digital farming, ends up hindering innovation rather than enhancing the widest data sharing[36].

On another ground, true that the 2019 Guidelines allow for the broadest differentiation of CoC disciplining the processing of personal data (which have the highest commercial value for business users); however, as highlighted in previous work, such disclosures may not be effective as they do not indulge on the different capabilities of recipients to such information to understand and process the meaning of algorithmic decisions done

[33] Unlike with international CoCs, the adoption of national ones is less complex: once submitted to the national SA, a preliminary formal control is made, following which – failing any exceptions – a decision on approval is made that is compliant with the national legal timeframe. A second decision on the merit is made by the SA that can either make comments on the draft CoC (and the proponents can accept or re-submit) or definitely approve it. Once approved, the CoC is made publicly available on both the SA's and the EDPS' Board's websites (Arts. 40(6) and 40(11) GDPR).

[34] According to Art. 83(2), GDPR and following EDPB (2018b), the adoption of CoC may lead to the application of no fine at all, should the SA consider that the corrective measures applied by the monitoring body are sufficient.

[35] Note 27 - le note nella versione originale sono fuori ordine dalla 19 si passa alla 21

[36] Graef, Gellert, and Husovec (2018) at 12 (stating that somehow contradictorily, on the one hand, the CoC 'pretends to facilitate the sharing of [non-personal] data by reinforcing the rights of the data originator [i.e. the digital farmer]. On the other hand, however, it provides for more restrictions to the free flow of data than would seemingly apply under the GDPR for personal data.').

by platforms and their consequences (Di Porto & Maggiolino, 2019, at 2)[37]. The only reference one can find is at pt. 28, where code owners are called to demonstrate that an appropriate level of consultation with the relevant stakeholders[38] over the draft Code has taken place. However, that does not say much on 'how' to assess the understandability and thus the efficacy of CoC.

More generally, there are several limitations on relying on 'encouraged' self-regulation, even where CoCs are conceptualized following the best existing practices. First, there is no guarantee that platforms will cooperate in setting or adhering to an industrywide code, even where the right incentives are set. Second, self-regulation in the digital society faces the limits of territorial oversight: provided (but not demonstrated) that an optimal control system is in place, it would necessarily act at a local (European) level, while platforms operate trans-nationally being their business data-driven. Therefore, as purported by Piffault, systemic risks, like those that occurred in the 2007 financial crisis, could repeat (Piffaut, 2018, p. 4).

Finally, self-regulatory approaches like those described above, do not put any constraint on the risk that platforms consolidate their economic power vis-à-vis their business counterparts, in particular by using self-regulation to raise regulatory barriers to entry of competitors (Finck, 2017, at 15).

Given these limitations, co-regulation has been suggested as a viable alternative to differently combine the ability of platforms to set micro standards with a higher degree of interference by public institutions.

4. *(Follows) The European model: Experimenting with (traditional) disclosure co-regulation: Regulation EU 2019/1150*

A second setting is disclosure co-regulation. Very broadly, co-regulation (Ayres & Braithwaite, 1994; Baldwin, Cave & Lodge, 2012, p. 146)[39]

[37] See also Taeihagh, *Introductory paper*, 9: 'As individuals either lack sufficient technical literacy or are not willing to bear the expected costs of obtaining the required information to interpret these explanations, mandated explanations required by the GDPR are unlikely to effectively inform and empower data subjects'.

[38] And the relevant stakeholders might include the platform's business users as 'data subjects or associations/bodies representing them'.

[39] We use the definitions given by Ayres and Braithwaite (1994) and Baldwin et al. (2012) 146: co-regulation is an 'industry-association self-regulation with some oversight and/or ratification by government.' Note that co-regulation is explicitly referred to in

encompasses diverse models, whereby a pool of decision-makers (the State, markets and technology intermediators) interact to produce policy, draft rules (laws, regulations, norms); review and oversee[40].

Differently from self-regulatory schemes described above, here the regulators' involvement serves the function of ensuring the achievement of some public objectives.

However, depending on the degree of contribution of platforms as regulatory intermediators, different configurations of co-regulation are possible (Marsden, 2011; de Streel & Sibony 2017, p. 22). In the following, we describe hybrid governance models (Radu this issue, 9–10) that are emerging as a consequence of the adoption of several piece of EU legislation in the field of digital disclosure regulation.

4.1. *EU regulation 2019/1150 on fairness and transparency of P2B relations*

An excellent example of disclosure co-regulation is that provided for in EU Regulation 2019/1150[41].42 To enhance transparency in the P2B relationships[42], the Regulation sets up a co-regulatory regime, where the *regulatory* part consists of 'a set of legally binding transparency obligations on platforms', while the *self-regulatory* one, of 'a non-binding call [to platforms] to establish an independent mediation body' for the out-of-court settlement of complaints[43]. In addition 'an EU observatory for

the two Communications by the Commission: EC (2016, February 2nd) and EC (2016, May 25th).

[40] So called meta-regulation (ie. the involvement of public authorities stands especially on the review/audit side, and external controls by the regulator serve to ensure compliance to internally-crafted rules) (Parker, 2002, 2005; Grabosky, 1995; contra Black, 2007; Scott, 2012. Coglianese & Lazer, 2003; Coglianese & Mendelson, 2010).

[41] See, above, note 5.

[42] According to EC, (2019), Regulation 2019/1150 has been adopted in response to various harmful trading practices realized by the platforms, such as: unilateral change of contractual terms and conditions without prior notice; delisting of goods or services; suspension of business users' accounts without a clear statement of reasons. Other practices related to transparency duties include: the setting of unclear conditions for access and use of the data generated and collected by the platform providers; lack of transparency in the ranking of goods and services; and the discriminatory treatment platforms reserve to providers, as compared to their own (competing) services. Finally, the EC contests that most-favoured-nation clauses have been widely used by the online platforms that restrict their couterparts' ability to offer more attractive conditions through other channels.

[43] See the Executive summary of the Impact Assessment (SWD (2018) 139 fin.) accom-

emerging problems, organized around an EU expert group' is set up 'to *monitor* emerging trends and the evolution of problems'.

Turning to the legally binding disclosure obligations, to curb surprise and increase the predictability of platforms' practices, terms and conditions must include information to the business users regarding significant contractual changes in clear, layman language and grant them a minimum (15 days) grace period (Art. 3). To prevent accidents like that of 2018, when 'Amazon blocked more than 250,000 seller accounts permanently and over 30,000 accounts temporarily,' (Westerhoff, 2019) platforms must state reasons for restricting, suspending or terminating trader users' services (with 30 days of prior notice) (Art. 4). Discrimination practices (i.e. platforms favouring their business or related commercial partners) are also subject to disclosure duties (Art. 6); and platforms shall describe rules on access (or non-access) to personal and non-personal data which business users provide to them or which are generated through the platform's use (Art. 7). This does not grant data access or portability to business users[44]; which are the subject of other rights under either the GDPR, the Regulation on the free flow of non-personal data, or other special regimes.

More transparency obligations are addressed to online general search engines, aimed at tackling the economic dependency induced by potentially harmful ranking practices[45]. Search engines are thus subject to a scoped transparency obligation to provide a 'description of the *main ranking parameters* and of the possibilities to influence such rankings against remuneration' (so-called pay-for-ranking results: Art. 5). Such obligations can be viewed as a form of rules that extend the 'explicability duties' (Arts 13 and 14, GDPR) from P2C to P2B relationships. By it, the 'logic' inspiring algorithmic decisions taken by the platforms should be made transparent and therefore accountable to the business. Of course,

panying the Proposal, at 2. Besides that, the Proposed Regulation foresees: on the regulatory side: 'an obligation to set up internal redress mechanisms, as well as provisions to allow for collective redress for associations representing businesses'.

[44] Graef et al. (note 63), at 11: 'While such obligations are a welcome step in creating transparency about the extent to which access to data is offered to business users, the proposed Regulation does not prescribe a minimum level of data access or ban any unfair practices relating to data access. As such, it does not tackle the interaction of data access with data protection in strategic behaviour that can undermine the level of data innovation to the detriment of both businesses and consumers.'

[45] Legal standing is awarded to organizations representing platforms' business counterparts (that can act on behalf of their members): see Executive summary of the Impact Assessment, cit., 2.

such an obligation does not imply any duty to disclose algorithms (usually configured as trade secrets).

4.2. *Critical assessment: is it really disclosure co-regulation?*

Overall, the strategy envisaged by Regulation 2019/1150 is a classical horizontal, undifferentiated, and light-touch disclosure self-regulatory one, despite the existence of the hard '*regulatory*' part, the mechanism for complaint-handling and the collective redress[46]. That is confirmed by the weak enforcement apparatus, where only monitoring tools – the voluntary mediation bodies – are envisaged vis-à-vis the infringement of analyzed disclosures[47].

If light enforcement might ensure broader cooperation of the platform players, it might, at the same time, spur distrust among the business users[48]. Similarly, the Regulation seeks platforms' cooperation by leveraging on their reputation (e.g. it requires platforms to disclose, on an annual basis, information about the effectiveness of their internal complaint-handling systems). If that obligation can enhance trust among consumers vis-à-vis the most consolidated players, it can nonetheless marginalize start-up platforms whose reputation is still in the making.

Considering the beneficiaries of the information disclosed, micro and SMEs are not the big business: not from an economic point of view, nor a legal one. SMEs tend to be 'economically dependent' by the platforms and search engines they operate through; and that explains why in some jurisdictions, like Germany, concurrent norms like abuse of economic dependence (or relative market power) apply along with Regulation 2019/1150 (Di Porto & Posdzun, 2018). Similarly, both Directives on Unfair Commercial Practices (UCP) and Unfair Terms and Conditions (UCT) continue to apply to SMEs operating in platforms (e.g. preventing

[46] See Annex to the IA, at 20 specifying that the costs for setting up the internal mechanism for complaint-handling and collective redress (following Arts. 9 and 12) towards platforms' business users should be 'minute' (Ibid, at 142).

[47] According to Art. 10, platforms are subject to a non-binding obligation to set up independent mediation bodies for out of court settlement; while monitoring is under the responsibility of an EU Observatory on the Online Platform Economy (which merely 'monitors' the impacts of the Regulation and its regulatory and self-regulatory components on the platforms economy).

[48] Even though there might be some spillover effects, as business users may utilize the legal provisions in court or antitrust proceedings (e.g. to help demonstrate discriminatory behavior by dominant platforms). See Annexes to the IA, at 144.

information manipulation)[49] even though they are not stricto *sensu* final consumers.

Finally, what the Regulation fails to recognize is that SMEs and especially microbusiness behave much like individuals, and therefore may suffer the same cognitive bias.

It instead accounts for a relatively typological, notional idea of SME, in support of which it offers the 'informational panacea'. Once again, when it comes to 'how' to draft information for the business users, the Regulation relies on 'codes of conduct' that the Commission shall 'encourage' platforms and search engines to draw up, without any further guidance (Art. 13). Requirements of simplification of information (and possibly salience) would be much welcome, such as those foreseen in Article 5 (description of ranking parameters).

However, fostering high levels of informational 'visibility' in the digital markets does not lead to increased transparency: quite the opposite, it conduces to decreased transparency and increased opacity (it is the so-called 'transparency paradox') (Stohl et al., 2016, p. 131).

In an aim to fill the design gap as far as the disclosures are concerned, other models of disclosure co-regulation in the P2B relations have been suggested that make greater use of the algorithmic decisional capabilities of platforms and their regulatory powers.

5. *New governance models: Data-based (or savvy) self- and co-regulation*

Including digital platforms' intermediation in the regulatory governance conundrum is the real advancement of more recent proposals. They dispose of mass regulatory and oversight capabilities that lack modern regulators for producing and implementing disclosures (Westerhoff, P. 2019).

Piffaut suggests that platforms be subject to a 'form of data-based regulation, where public policy objectives are attributed to them, and their achievement validated through data analysis'. (Piffault, at 2) In his view, some form of smart regulation, that he terms 'savvy regulation', should be put in place starting from the consideration that digital platforms are foremost 'run on the basis of and produce data'. Therefore, they can

[49] To mention an example, in Italy Facebook has been condemned for providing misleading information under the UCP regime, and the Competition Authority (which is responsible for applying such set of rules), applied a €10 Mlo administrative fine.

perform better than traditional regulators, provided that they possess the infrastructure and data needed to both draft differentiated rules and oversee their implementation at a very granular level. They also have an incentive to do so, given that the more effective their oversight, the higher their reputation. That would put platforms in the best position to also address negative issues showing some public interest like, for instance, tax evasion or green rules compliance in flat renting[50].

On that basis, the author suggests putting an obligation onto platforms to provide the regulator with 'access to data and to allow simulations to satisfy compliance with some predetermined [public interest] standards' (Piffault at 6). In particular, once the pursuit of a public objective is assigned to a platform (e.g. avoiding discrimination between hosts in an accommodation application), data feeding the algorithms used by the platforms should be made accessible to the regulator and the wider public to allow testing and ensure compliance with some pre-determined standards.

The proposal points to a fairly open access regime, where the public interest issue at stake is openly discussed, and the data generated by the platform are made publicly accessible to allow third parties (the academia included) 'to test ideas and adaptations, conduct experiments and use the collective intelligence instead of sticking to proprietary private data'[51]. Obviously, one can expect fierce opposition by the platforms to the sharing of 'large quantities of behaviour-revealing data with public authorities' (Finck, 2017, at 13).

At the other side of the (ideal) spectrum stands Sundararajan, (EP, 2017) who purports a 'data-driven delegation' model. Here, 'data is instead left inside the platform's systems while allowing [its] use for regulation by delegating regulatory responsibility to the platform.'

Concerning controls, audits that are needed to check for compliance would be supplemented by an API; the latter, however, 'would not provide access to raw data, as in Piffault's model, but could allow a government to run "queries" to verify compliance.[52]' For instance, APIs could randomly check for compliance of tax collection by platforms.

The core of Sundararajan's proposal is that platforms are the only ones to own the data and the capacity to run analytics over big datasets that

[50] As reported by the EP (2017), at 24, the City of Lisbon delegates the hotel occupancy tax collection to AirBnB. In the same vein, a Municipality could delegate AirBnB with the implementation of environmental rules on differentiated home waste collection, e.g. by nudging homeowners through higher ranking positions.

[51] Ibid. at 7.

[52] Ibid.

are relevant for regulatory purposes. Also, they are in the best position to check for discrimination, biases and other undesired consequences of (their own) algorithmic decisions. Therefore, 'rather than tasking the government with the development of such methods on data provided by platforms, it is better to allow, or perhaps even require, the platforms to develop these methods themselves and apply these to the data that remains within the platforms. After all, they have access to some of the world's best computer scientists[53].'

Although it is undeniable that governments do not possess the technical capabilities to duly oversee platforms' algorithmic regulatory powers, the proposal completely dismisses the quests made by the Council of Europe and the EP – which happens to be the same editor as that of Sundararajan's proposal[54]. It is worth reminding that the latter have been calling for the activation of empowerment strategies, 'supported by AI tools'[55], to countervail the manipulative potential of AI-led decisions.

6. *Algorithmic disclosure co-regulation for platforms' business users*

In view to empower small business users through AI tools and also strengthening the accountability of platforms' decision-making as far as disclosures are concerned, we suggest endorsing algorithmic disclosure co-regulation. Building on previous work[56], we will articulate on how this model also answers the quest for increased participation[57] of business users in algorithmic decisions that affect their economic lives, without having to receive the disclosures passively. Our model provides a cost-effective way to carry on frequent assessment on datasets to produce well-functioning algorithmic disclosures on a collaborative fashion, instead of delegating this task completely to the platforms.

Our model is based on three propositions and starts from a set of observations. The propositions are: (1) that disclosures targeted at business users should be done by algorithms (as suggested by the EP); (2) should be pre-tested in a co-regulatory process that involves the regulator (possibly the European Commission, the Berec or an ad hoc EU authority enjoying

[53] Ibid. at 25.
[54] See above, the Introduction.
[55] EP (2019 Jan.) at 7.
[56] Di Porto & Maggiolino (2019).
[57] EP (2019 Apr).

enforcing powers), the platforms, the business users and the consumers (using regulatory sandboxes); and (3) enforced through legal and other empowerment tools, rather than sole fines.

As far as the observations are concerned, our starting point is the EDPB's important statement (2018a), according to which: algorithms are subject to bias and 'can result in assessments based on imprecise projections'. (p. 27) Therefore, it is crucial to 'carry out frequent assessments on the data sets . . . to check for any bias, and develop ways to address any prejudicial elements, including overreliance on correlations'. Those checks and audits require 'regular reviews of the accuracy and relevance of automated decisionmaking, including profiling . . . not only at the design stage but also continuously' (p. 28). This affects algorithms used by platforms, which are subject to frequent changes to provide for the best products and services. And makes EU legislative duty to disclose the 'main parameters' of algorithmic rankings[58] of little value for business users, because such parameters can become rapidly obsolescent, making their disclosure not timely, or the chosen format outdated or its content meaningless. Therefore, instead of requesting the platforms to provide for access to their data or their algorithms, we suggest instead that the disclosure duties to which they are subject (which may regard ranking parameters but also other contractual clauses), be drafted in a completely different fashion.

For any disclosure targeted at business users in platforms to be tailored at their informational needs, meaningful and dynamic (i.e. changing over time according to their preferences), we propose to set up an agile group for the ex-ante testing of algorithmic disclosures in the course of a co-regulatory process[59]. That is, in fact, not entirely new to the regulatory landscape, as 'regulatory sandboxes' already exist in the Fintech industry, where new rules are experimented in controlled environments (thanks to simulations run over big data) before being implemented at large scale[60].

The envisaged small experimental group would include the regulator (that takes the initiative, like in innovation hubs), the final consumers

[58] See Recitals 26–28 and art. 5, Regulation EU 1150/2019 requiring search engines to disclose the 'description of the main parameters determining the ranking of all indexed websites and their relative importance'.

[59] (Gahnberg, pp. 9–10).

[60] Regulatory sandboxes are aimed at fostering collaboration between regulators and the financial industry to test new regulations in controlled environments (check their potential impacts on consumers and the market) before implementation. That, in turn, helps to foster innovation in the Fintech industry. See: ESMA, EBA and EIOPA (2019); Piri (2019); Arner et al. (2016), Mattli (2018); Picht and Loderer (2018).

and individuals representing the platforms and the SMEs. The actual individuals representing the SMEs would of course vary depending on the topic of algorithmic disclosures (for instance, if layouts to be tested in the sandbox through algorithms pertain to how to share data in the short-term rental sector, then participants in the sandbox would be digital platforms operating in there, flat owners, consumers, data scientist technicians, and the regulator)[61].

Goal of the group would be to train the selected algorithm for designing the disclosures. So for instance, when drafting different disclosure formats of 'the main parameters determining the ranking of all indexed websites and their relative importance', Art. 5 Regulation EU 1150/2019 requires that search engines allow corporate website users to 'obtain an adequate understanding' of 'whether, and how and to what extent, certain design characteristics of the[ir] website. is taken into account' by the algorithm in its ranking. Hence, pre-testing in a controlled environment the best format such information might have, that is also produced automatically through an algorithm and fairly accommodates the interests of all stakeholders is a desirable outcome.

The testing would also allow to comply with a further legal requirement, namely: to 'ensure predictability for corporate website users', not of the parameters though, but of the disclosures; while also ensuring that 'the description. be kept up to date, including the possibility that any changes to the main parameters should be made easily identifiable.' (Art. 5). In our proposal, diverse algorithmic techniques[62] would be used to develop disclosures that are differentiated and targeted at various groups of SMEs depending on their willingness to receive a more simplified or granular (detailed) disclosure format (e.g. three groups may be identified while running the tests: (i) simple, (ii) intermediate, and (iii) sophisticate recipient)[63]. Every choice they make will be tracked during the test, and data will feed the algorithm, providing it with information on how to

[61] It is especially important to select these stakeholders in a way that the interests of the business users are well represented before those of the platforms and enough receptive of those of final consumers

[62] Several algorithmic techniques exist (think of Natural Language Processing – NLP – or Generation – NLG) that allow for text mining and simplification, but also the graphic rendering of text (super or hyper-simplification).

[63] Based on data, 'clustered' disclosures can be produced that meet the needs of the recipients, while adapting to the changing of their preference over time. For instance, over-simplified information about the ranking parameters could
[b]e provided, that are clustered (i.e. based on a group of users with similar characteristics).

produce the best disclosures, meaning those that fail the least to be read, understood and give a due course of action. Technically speaking, we suggest using a knowledge graph to realize the differentiated targeted disclosures. The process should start with three libraries: two of which are textual (the disclosure duties established by EU laws and regulation; and the platforms' disclaimers implementing them), and one would consist of the behavioural data coming from the sandbox. In conceptualizing the sandbox, we should elaborate on the concepts that are typical of one sector. To do so, we need to create relationships with a natural language sandbox: that serves to allow humans to participate in the sandbox to either confirm or reject such concepts. On that basis, we should produce them to all the stakeholders in the sandbox (because we are in a co-regulatory regime). By saying that they are 'satisfied' (i.e. by 'confirming' the layouts), they will feed into the sandbox.

We should reproduce that test for several formats and several times (sessions) until we get to the point where all participants are mostly satisfied and least dissatisfied. We should repeat this with the clauses of each disclosure per each of the 3 or n formats we want to target the cluster SMEs.

In the knowledge graph, both the texts and behavioral data would be integrated employing SMEs' user experience[64]. Behavioral data coming from the regulatory sandbox would be used to confirm or contradict the links described by the graph[65].

The human presence, as said, is essential to monitor if errors occur in the building of the knowledge graph: technicians supervising in the

[64] To make a parallel, this operation resembles the way Google search engine operates (through domains and supradomains). More specifically, when Google users are shown a picture and are asked to 'confirm' that what they see is a cat, they can confirm or not. If they do, they reinforce a node of the graph (that the picture shown is a cat and not, say, a muffin). Similarly, human stakeholders in the sandbox provide behavioral data that confirm a proposed clause or text, thus reinforcing nodes, and gradually strengthening the links in our knowledge graph.

[65] The ontology serves to link all the pieces with concepts of the domain, supra-domain, and vertical (i.e. sector-specific) domain. For instance, imagine we aim to link the term 'fintech' (domain) to the normative goal (supra-domain) to a sector-specific term, like 'transparency in financial fintech' (vertical domain). However, because most of the time, norms do not speak in such a detail, we need to use a meta-level to provide further instructions. For instance, very often norms in the financial domain do not require retailers of financial products to disclaim full detailed composition of their products, but would instead require for general transparency. Therefore, we would need to provide a meta-level whereby to instruct the algorithm this way: 'When using the word 'norms', link it to the concept 'transparency', then link it to 'disclaimer'.

sandbox may intervene to eventually deactivate any error that may occur in the algorithm. That implies that we need technicians to participate in the sandbox, besides regulators, firms (platforms and SMEs), and consumers.

It is important to stress that there would be no need for the platform to disclose any of its own algorithms (which might easily remain secret) to other stakeholders participating in the trials[66].67 That is because the kinds of algorithms that are needed to get to targeted algorithmic disclosures are either available on an open access basis[67], or because it could be provided by the regulator itself (Di Porto 2020). The consumers and SMEs contribute with their behavioral data to feed the algorithm: for instance, in case of disclosures of standard form contracts (typically the fine print one finds online and hardly reads), the experimental phase would consist of the stakeholders testing different formats of ToCs[68].

Testing is also relevant to implement rapid amendments to the algorithmic disclosures, should any major risks associated with AI-led decisions emerge during the training (such as algorithmic biases in rankings, overreliance on correlation or discrimination).

Following the best practice identified by the Art. 29 WG, such modifications would feedback into the algorithm to ameliorate it and, consequently, the disclosures.

Indeed, the pre-testing phase also allows detecting with some precision what are the informational needs and understanding capabilities of the business users. In this sense, algorithmic disclosures would produce useful information, by dynamically adapting its content and format to what the recipient needs at the time she needs. Also, as articulated elsewhere, because co-regulated algorithmic disclosures would necessarily be targeted at the different informational needs of the recipients, they would comply with the principle of proportionality (Di Porto & Maggiolino 2019).

[66] Notoriously, algorithms are covered by IPRs (and are usually qualified as trade secrets). Legally speaking, under EU law firms are not entitled any general right to be informed about the overall system used to make automatic decisions, nor can they demand the full disclosure of the algorithm: see Recital 27 and Art 5(6) Regulation EU 1150/2019.

[67] Just to make an example, think to the very ambitious publicly-funded Lynx project (<http://lynx-project.eu/> (accessed on June 5, 2020), providing for an ontology of linked legal sources aimed at making compliance easy to firms (especially SMEs) in three legal domains (business law, labor law and energy law). For more details, see Montiel-Ponsoda & Rodríguez-Doncel (2018)

[68] Notoriously, algorithms are covered by IPRs (and are usually qualified as trade secrets). Legally speaking, under EU law, firms are not entitled to any general right to be informed about the overall system used to make automatic decisions, nor can they demand the full disclosure of the algorithm: see Recital 27 and Art 5(6) Regulation EU 1150/2019.

Once sufficient data is gathered that the tested algorithm can produce well-functioning disclosures, intended as those that are informative to the identified groups and biasfree (i.e. or not conducive to self-serving information manipulation), are algorithmic disclosures implemented on large scale.

The same is for any modification to the algorithmic disclosures that the participants to the sandbox accept – and the regulator certifies: they become implementable by the platforms on a large scale.

Also, they could be given a special legal effect: for instance, all pre-tested modifications could automatically be implemented and produce a direct effect among the counterparties.

So for instance, an amendment to the Terms of Contract of a certain service in a given sector, which is agreed upon in the sandbox, and implemented in the algorithmic disclosure, could become immediately effective.

With algorithmic disclosure co-regulation, enforcement of disclosures becomes somehow less problematic. Codes of conduct would no longer be a fictional substitute for compliance, as the effectiveness of disclosures to really inform recipients would be tested in advance.

7. *Discussion and conclusion*

In this paper, we reviewed different models that include digital platforms as regulatory intermediators, alongside the public authorities (at the EU level) and the markets. In this journey, we explored which one was best suited to build disclosure regulation for the platform economy, between 'solicited' or 'encouraged' self-regulation (based on codes of conduct) and co-regulation. In this latter case, we explored how technology, and AI algorithms, especially, could contribute to the shaping of a well-functioning co-regulatory system.

We concluded that none of the two 'extreme' proposals reviewed was suitable: not the fully open 'savvy option', mandating platforms to share the data feeding their algorithms with the wider public, because it would stifle innovation. Nor the 'data-delegated regulation' option, because it would not solve the problem of possible algorithmic manipulation by platform, identified as a significant concern by both the Council of Europe and European Parliament.

On our side, we proposed a regulatory sandbox model where

stakeholders come together to develop and train an algorithm that could provide disclosures about the platform's operations to the business-users.

We suggest that disclosures (still the core of EU legislation of digital platforms) be conceived and drafted through algorithms (algorithmic disclosures). That would necessarily imply a collaboration between the platforms and the regulator (as the other proposals) but would imply wider participation, by allowing also individuals representing final consumers and the SMEs to contribute in the design of disclosure. Algorithmic disclosures are thus pre-tested (by running analytics) in small groups representing all the mentioned stakeholders (like in regulatory sandboxes); freed of biases and risks of manipulations, through repeated testing and feedbacks and then implemented on a large scale.

We contended that not only do ex-ante design, testing and amendments of algorithmic disclosures increase participation of SMEs in the rule-making process, but they do also provide for greater empowerment to the business users. On this last point, lacking empirical evidence, one can only speculate that by actively receiving targeted and personalized disclosures, a business user will be better empowered that through undifferentiated, detailed, untimely information about, say, the 'main parameters determining the ranking' of its services.

One of the main problems is to ensure collaboration in the sandbox. Why should the platforms share their (private) algorithmic regulatory power with the public rule-maker and the addressees? And also, why would the digital firms want to participate in the regulatory sandbox instead of producing their own disclosures? In the end, anything that happens in the sandbox implies some disclosure of trade strategies to the regulator, competitors, and SMEs and final consumers. Information is an asset, and even in the little margins left by the disclosure duties, platforms might not want to share the way to convey it to their clients.

Setting the right incentives is pivotal to gain participation. First, there is a reputational advantage for the platforms, which are seen as engaging in pro-small business activities.

Second, the automatic production of rules saves the costs for producing the disclosures and updating them. Third, the direct effect of modifications of disclosures agreed in the sandbox does also save costs to the platforms. As per the incentives for SMEs and consumers, they will have voice and representation in the rule-making process by feeding the algorithm with their behavioral data.

Such disclosures would save costs on platforms and search engines for

not having to continually update their disclosures (like their terms and conditions on rankings) and to notify these changes to all their counterparts. As said, all disclosures and changes that are agreed upon in the sandbox will be directly implemented through the algorithm and would most probably generate less litigation in court. In this sense, algorithmic disclosures may save some costs of private enforcement, at least for the pre-tested issues, provided that they have been thoroughly discussed and accepted within the pre-trial, and certified by the regulator.

One should mention that not all domains are suitable for algorithmic disclosures. For instance, in some areas retailers might not use (or not use yet) algorithms or big data technologies, and cannot, therefore, take advantage of this new mode of disclosure.

Given that they would empower micro and SMEs, algorithmic disclosures may potentially help saving time for the scaling-up process of European digital companies.

Finally, the co-regulatory process entailed in such disclosures would maintain a leading role for the Commission, the Berec or a new EU-wide authority for algorithms. The EU, however, would still need to cooperate internationally to ensure that algorithmic disclosures might have a legal effect also outside its borders.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by the Lady Davis Fund and the Ministero dell'Istruzione, dell'Università e della Ricerca PRIN Project, 2017 Prot. 2017BAPSXF.

References

Abbot K. W., D. Levi-Faur & D. Snidal, *Theorizing regulatory intermediaries*, in *The ANNALS of the American Academy of Political and Social Science*, 670(1), 14, 2017.

Acquisti A., J. Grossklags, *What can behavioral economics teach us about privacy?* In A. Acquisti, S. Gritzalis, C. Lambirnoudakis, S. de Capitani di Vimercati (Eds.), Digital privacy: Theory, technologies

and practices. Auerbach Publications, 2007, p. 363.
Ananny M. & K. Crawford, *Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability*. New Media & Society, vol. 20(3), 973–989, 2016.
Argenton C. & J. Prüfer, *Search engine competition with network externalities*, in *Journal of Competition Law and Economics*, vol. 8(1), 73, 2012.
Arner D. W., J.N. Barberis, R.P. Buckley, (2016). *Fintech, RegTech, and the reconceptualization of financial regulation*, in *NW. Journal of International Law & Bus*, vol. 37, 371, 2016.
Ayres I. & J. Braithwaite, *Responsive regulation*. Oxford University Press, Oxford, 1994.
Baldwin R., M. Cave & M. Lodge, *Understanding regulation*. Oxford University Press, Oxford, 2012.
Ben-Shahar O. & C. E. Schneider, *The failure of mandated disclosure*, in *University of Pennsylvania Law Review*, vol. 159, 647, 2011.
Ben-Shahar O. & C. E. Schneider, *More than you wanted to know: The failure of mandated disclosure*. Princeton University Press, Princeton, 2014.
Black J., *Constitutionalising self-regulation*, in *The Modern Law Review*, vol. 59(1), 24, 1996.
Black J., *Decentring regulation: Understanding the role of regulation and self-regulation in a "post-regulatory" world*, in *Current Legal Problems*, vol. 54(1), 103, 2001.
Black J., *Tensions in the Regulatory State*, in *Public Law*, Spring, p. 58, 2007.
Busch C., *Crowdsourcing, consumer confidence: How to regulate online rating and review systems*, in C. Economy & A. De Franceschi (Eds.*), European contract law and the digital single market: The implications of the digital revolution* (p. 223). Intersentia, Uitgevers, 2016a.
Busch C., *The future of pre-contractual information duties: Personalization of disclosures with big data*. In Twigg-Flesner (Ed.), *Research handbook on EU consumer and contract law* (p. 221). Edward Elgar, Cheltenham. Retrieved from <http://ssrn.com/abstract=2728315>, 2016b.
Busch C. & A. De Franceschi, (2018). *Granular legal norms: Big data and the personalization of private law*. In V. Mak, E. Tjong Tjin, & T. A. Berlee (Eds.), *Research handbook on data science and law* (p. 408). Edward Elgar, Cheltenham. Retrieved from: <http://ssrn.com/abstract=3181914>, 2018.
Busch C., *Self-regulation and regulatory intermediation in the platform*

economy. In M. Cantero Gamito & H. W. Micklitz (Eds.), *The role of EU in transnational legal ordering* <http://ssrn.com/abstract=3309293>, 2019.

Coglianese C. & E. Mendelson, *Meta-regulation and self-regulation*. In R. Baldwin, M. Cave, & M. Lodge (Eds.), *The Oxford handbook of regulation* (p. 146). Oxford University Press, Oxford, 2010.

Coglianese C. & D. Lazer, *Management based regulation: Prescribing private management to achieve public goals*, in *Law Society Review*, vol. 37(4), 691, 2003.

Coglianese C. & D. Lehr, *Transparency and algorithmic governance*. Additional District Magistrate (LR), 71, 1, 2019.

Cohen M. & A. Sundararajan, *Self-regulation and innovation in the peer-to-peer sharing economy*, in *The University of Chicago Law Review*, 82, 116–131, 2015.

Council of Europe. Declaration by the committee of ministers on the manipulative capabilities of algorithmic processes. Decl(13/02/2019)1, 13.2.2019.

Craswell R., *Taking information seriously: Misrepresentation and nondisclosure in contract law and elsewhere*, in *Virginia Law Review*, vol. 92, 565, 2006.

de Streel, A., & Sibony, A.-L, *Towards smarter consumer protection rules for the digital society*. CERRE Project Report, 2017.

Di Porto, F., & Ghidini, G., *I access your data, you access mine. Requiring Data Reciprocity in Payment Services*. IIC, 51, 307–329, 2020.

Di Porto, F., & Maggiolino, M., *Algorithmic information disclosure by regulators and competition authorities*, in *Global Jurist*, 19(2), 1–17, 2019. Retrieved from: <http://ssrn.com/abstract=3363169>.

Di Porto, F., & Posdzun, R. (Eds.). *Abusive practices in competition law*, Ascola series, Edward Elgar, Cheltenham, 2018.

Di Porto, F., *From BADs to BEDs. Algorithmic Disclosure Regulation. Theoretical aspects for empirical application*, in Hebrew University of Jerusalem Legal Research Paper 20-18, 2020. Retrieved from: https://ssrn.com/abstract=3633847 or <http://dx.doi.org/10.2139/ssrn.3633847>.

Easterbrook, F. H., & Fischer, D. R., *Mandatory disclosure and the protection of investor*, in *Virginia Law Review*, 70(4), 669, 1984.

EC. Communication, *A European agenda for the collaborative economy*, COM(2016)0356 final, (2016a, February 2nd).

EC. Communication, *Online platforms and the digital single market*, COM

(2016) 288 final, (2016b, May 25th).
EC. Communication, *Building a European data economy*, COM(2017)9 fin., 10. 1, 2017.
EC. Communication, *Towards a common European data space*, COM(2018)232 final, 2018.
EC. *Competition policy for the digital era*. Report by J. Crémer, Y.-A. de Montjoye, H. Schweitzer, 16, 2019.
EC. Communication on *A European strategy for data* (COM(2020) 66 final), 2020a, <https://eurlex.europa.eu/legal-content/EN/TXT/?qid=1601713734544&uri=CELEX:52020DC0066>
EC. *Shaping Europe's digital future*. (COM(2020) 67 final), 2020b <https://eur-lex.europa.eu/legalcontent/EN/TXT/?qid=1601713734544&uri=CELEX:52020DC0067>
EC. *White paper on AI*. (COM(2020) 65 final), 2020c. <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1601713734544&uri=CELEX:52020DC0065>
EC. *Digital Services Act package: Ex ante regulatory instrument for large online platforms with significant network effects acting as gate-keepers in the European Union's internal market, Inception impact assessment*, Ares(2020)2877647, 4 June, 2020d.
EDPB - European Data Protection Board. *Guidelines on automated individual decisionmaking and profiling*, 6 February, 2018a.
EDPS - European Data Protection Supervisor. *Guidelines 1/2019 on codes of conduct and monitoring bodies under regulation 2016/679*, 12 February, 2019.
ESMA, EBA and EIOPA. *FinTech: Regulatory sandboxes and innovation hubs*, JC 2018 74, 2019.
European Commission. Communication, *A digital single market strategy for Europe*. COM (2015)192 fin., 6. 5.2015.
EU High-level Expert on AI. *Ethics guidelines for trustworthy AI*. (April 8, 2019).
European Parliament (EP). *The collaborative economy: Socioeconomic, regulatory and policy issues,* (by A. Sundararajan), PE 595.360 EN, IP/A/IMCO/2016-12, February, 2017.
European Parliament (EP). *A governance for algorithmic accountability and transparency*, PE624.262, April. 2019b
European Parliament (EP). *Artificial intelligence: Challenges for EU citizens and consumers*, PE631.043, January, 2019a.
Evans, D. S., & Schmalensee, R., *The antitrust analysis of multisided*

platform businesses, in R. D. Blair & D. D. Sokol (Eds.*), The Oxford handbook of international antitrust economics*, p. 404. Oxford University Press, Oxford, 2015.

Evans, D. S., & Schmalensee, R., *Matchmakers: The new economics of multisided platforms*, Harvard Business Review Press, Boston, 2016.

Finck, M., *Digital regulation*, in *LSE Law, Society and Economy Working Paper* 15/2017, 2017.

Gal, M. S., *Algorithmic Challenges to Autonomous Choice*, in *Michigan Telecommunication and Technology Law Review*, vol. 25, 59–104, 2017.

Gahnberg, C., *The governance of artificial agency,* in *Policy* & Society, 2020.

Gaudeul, A., & Jullien, B., *E-commerce, two-sided markets and info-mediationi*, in E. Brousseau & N. Curien (Eds.), *Internet and digital economics,* p. 268. Cambridge University Press, Cambridge, 2008.

Grabosky, P. N., *Using non-governmental resources to foster regulatory compliance*, in *Governance*, 8(4), 527, 1995.

Graef, I., Gellert, R., & Husovec, M., *Towards a holistic regulatory approach for the European data economy: Why the illusive notion of non-personal data is counterproductive to data innovation*. DP 2018-028 TILEC Discussion Paper, 2018. Retrieved from <http://ssrn.com/abstract=3256189>.

Grunes, A. P., *Another look at privacy*, in *The George Mason Law Review*, vol. 20, 1107, 2013.

Hagel, J., & Rayport, J. F., *The coming battle for customer information*, in *Harvard Business Review*, 53–61, 1997.

Heemsbergen, L., *From radical transparency to radical disclosure: Reconfiguring (in) voluntary transparency through the management of visibilities*, in *International Journal of Communication*, vol. 10, 138–151, 2016.

Lessig, L., *Code and other laws of cyberspace*. Basic Books, New York, 1999.

Lim, H. S. M., & Taeihagh, A., (2019). *Algorithmic decision-making, in AVs: Understanding ethical and technical concerns for smart cities*, in *Sustainability*, vol. 11(20), 5791, 2019.

Marotta-Wrugler, F., *Even more than you wanted to know about the failures of disclosure*, in *NYU L. and Econ. Working Papers*, Paper n. 394, 2014. Retrieved from <http://lsr.nellco.org/nyu_lewp/394>

Marsden, C., *Internet co-regulation*. Cambridge University Press, Cambridge, 2011.

Mattli, W. (ed.)., *Global algorithmic capital markets: High-frequency*

trading, dark pools, and regulatory challenges. Oxford University Press, Oxford, 2018.

Medzini, R., *Regulatory Intermediaries in the European privacy regime: How, why and to what effect*?, 2018. Retrieved from <https://csrcl.huji.ac.il/event/rotem-medzini>

Montiel-Ponsoda, E., & Rodríguez-Doncel, V., *Lynx: Building the legal knowledge graph for smart compliance services in multilingual Europe*. In G. Rehm, V. Rodríguez-Doncel, & J. Moreno-Schneider (Eds.), *Proceedings of the 1st workshop on LREC (language resources and technologies for the legal knowledge graph) workshop* (2018, May 12), pp. 19–22. Retrieved from <https://delicias.dia.fi.upm.es/members/vrodriguez/pdf/2018.legalkg.pdf>

OECD, *Rethinking antitrust tools for multi-sided platforms*, 2018. Retrieved from <http://www.oecd.org/competition/rethinking-antitrust-toolds-for-multi-sided-platforms.htm>

OECD, *Recommendation on AI*. Paris, 2019.

Parker, C., *The open corporation: Effective self-regulation and democracy*, 2002. Cambridge University Press, Cambridge.

Parker, C., *Regulator-required corporate compliance program audits*, in *Law Policy*, vol. 25(3), 221, 2005.

Picht, P. G., & Loderer, G. T., *Framing algorithms – competition law and (other) regulatory tools*, in MPI Research Paper No. 18-24. Retrieved from <http://ssrn.com/abstract=3275198>

Piffaut, H., *Platforms, A call for data-based regulation*, in CPI Antitrust Chronicle, 4., 2018

Piri, M.M., *The changing landscapes of fintech and regtech: Why the United States should create a federal regulatory sandbox*, in *Business and Finance Law Review*, 2, 233–254, 2019.

Prat, A., *The wrong kind of transparency*, in *American Economic Review*, 95(3), 862, 2005.

Radu, R., *AI governance: National, hybrid, ambiguous*, in *Policy & Society*, 2020.

Rust, R. T., Kannan, P. K., & Peng, N., *The customer economics of internet privacy*, in *Journal of the Academy of Marketing Science*, 30(4), 455, 2002.

Scott, C., *Regulating everything: From mega- to meta-regulation*, in *Administration*, vol. 60, 57, 2012.

Shelanski, H. A., *Information, innovation, and competition policy for the internet*, in *University of Pennsylvania Law Review*, vol. 161, 1663, 2013.

Special issue of Reg.&Gov, *Exploring the formal and informal roles of*

regulatory intermediaries in transnational multi stakeholder regulation, pp. 125–298, 2019.

Stohl, C., Stohl, M., & Leonardi, P. M., *Managing opacity: Information visibility and the paradox of transparency in the digital age*, in *International Journal of Communication*, 10, 123–137, 2016.

Strahilevitz, L., & Porat, A, *Personalizing default rules and disclosures with big data*, in *Michigan Law Review*, vol. 112, 1417, 2014.

Susser, D., Roessler, B., & Nissenbaum, H., *Technology, autonomy, and manipulation*, in *Internet Policy Review*, 8, 2–3, 2019.

Taeihagh, A., *The governance of artificial intelligence and robotics*, in *Policy & Society*, 2020.

Tan, S., & Taeihagh, A., *Governing the adoption of robotics and autonomous systems in long-term care in Singapore*, in *Policy & Society*, 1–21, 2020. doi:10.1080/14494035.2020.1782627

The Stigler Center Group at Chicago Booth, *Report by the committee for the study of digital platforms, privacy and data protection subcommittee*, 2019. Retrieved from <https://research.chicagobooth.edu/-/media/research/stigler/pdfs/data—report.pdf?la=en&hash=54ABA86A7A50C926458B5D44FBAAB83D673DB412>

Tirole, J., *Economics for the common good*, 2017. Oxford, Oxford University Press.

U.S. Federal Trade Commission (FTC), *The sharing economy*, FTC staff report, 2016. Retrieved from <http://www.ftc.gov/system/files/documents/reports/sharing-economy-issues-facingplatforms-participants-regulators-federal-trade-commission-staff/p151200_ftc_staff_report_on_the_sharing_economy.pdf>

U.S. Office of Science and Technology, Draft memorandum for the heads of executive departments and agencies. *Guidance for Regulation of Artificial Intelligence Applications*, 2020. Retrieved from <http://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMBMemo-on-Regulation-of-AI-1-7-19.pdf>

Vaidhyanathan, S., *The googlization of everything (and why we should worry)*, Los Angeles: Univ. of California Press, 2011.

Westerhoff, P., *The German Amazon marketplace agreement case: A landmark settlement with global reach or more hype than substance?*, 20.11.2019, 2019. Retrieved from: <http://www.hausfeld.com/news-press/the-german-amazon-marketplace-agreement-case-a-landmark-settlementwith-global-reach-or-more-hype-than-substance>

Whittington, J., & Hoofnagle, C. J., *Social networks and the law:*

Unpacking privacy's price. North Carolina Law Review, vol. 90, 1327, 2012.

Zuboff, D., *The age of surveillance capitalism: The fight for the future at the new frontier of power*. New York: Public Affairs, 2019.

Daniel Foà

Open banking*:*
API, accesso ai conti e nuove commodities *nell'era digitale*

1. *Introduzione*

La Direttiva dell'Unione europea 2015/2366 (PSD2) ha modificato profondamente la materia dei servizi di pagamento, già disciplinata dalla Direttiva 2007/64, anche regolando nuove tipologie di operatori che si caratterizzano per la prestazione di servizi innovativi: gli AISP (*Account Information Service Providers*) e i PISP (*Payment Initiation Service Providers*)[1]. Tra le novità introdotte dalla PSD2 che hanno avuto il più ampio risalto – e hanno maggiori potenzialità economiche – deve certamente annoverarsi l'obbligo imposto alle banche di rendere accessibili a soggetti terzi alcuni dati in proprio possesso. Si tratta della c.d. *access to account rule*, che ha la sua fonte nell'art. 36 della direttiva.

Con l'introduzione della disciplina di nuove figure di prestatori di servizi di pagamento si è ampliata la nozione di servizio di pagamento, ricomprendendovi anche ipotesi in cui l'intermediario non operi alcun trasferimento di somme di denaro né gestisca conti di pagamento[2]. Difatti,

---

* Questo articolo è stato originariamente pubblicato in A. Nuzzo (a cura di), *Blockchain, smart technologies and market governance*, LUISS University Press, Roma, 2022, pp. 37 e ss.

[1] Un ulteriore servizio – già diffuso nella prassi – tipizzato dalla direttiva è il *fund checking* svolto dai *Card Issuer Credit Providers*.

[2] Si vedano sul punto, tra gli altri, M. Rabitti e A. Sciarrone Alibrandi, *I servizi di pagamento tra PSD2 e GDPR: open banking e conseguenze per la clientela*, in F. Capriglione (a cura di) *Liber Amicorum per Guido Alpa*, Padova, 2019; F. Maimeri e M. Mancini (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, Quaderni di Ricerca Giuridica della Consulenza Legale della Banca d'Italia, n. 87, settembre 2019; A. Burchi, S. Mezzacapo, P. Musile Tanzi, V. Troiano, *Financial Data Aggregation e Account Information Services. Questioni regolamentari e profili di business*, Quaderni FinTech 4/2019, <http://www.consob.it>; M.C. Paglietti, M.I. Vangelisti (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento di interessi nella PSD2*, Roma, 2020; B. Russo, *L'evoluzione dei sistemi e dei servizi di pagamento nell'era digitale. Atti del Convegno nazionale in ricordo del Prof. Giuseppe Restuccia*, Padova, 2020.

i c.d. *Third Party Providers* svolgono attività che consistono, perlopiù, nell'aggregazione

di dati e nella trasmissione di ordini di pagamento, per lo svolgimento delle quali non è necessario che il cliente apra un apposito conto di pagamento presso il TPP[3].

Con finalità chiaramente pro-concorrenziale, è stato quindi garantito agli AISP e ai PISP il diritto di accedere a dati ed informazioni, relativi ai conti di pagamento tenuti presso le banche e gli altri prestatori dei servizi di radicamento dei conti di pagamento (*incumbents* del settore), necessari per la prestazione dei propri servizi alla clientela, quando i clienti vi acconsentano[4].

Indagando le *rationes* di siffatte innovazioni, da un lato emerge come la disciplina dei servizi di *account information* e *payment initiation* risponda all'esigenza di continuare a garantire un effettivo *level playing field* (nonostante le rapide innovazione tecnologiche rischino di sottrarre talune attività alla regolazione, impedendo l'effettiva applicazione della regola "same risks, same rules"[5]); dall'altro, il legislatore ha inteso evitare che agli operatori non bancari fosse preclusa la possibilità di erogare determinati servizi per i quali è necessaria la disponibilità dei dati bancari dei clienti. È, peraltro, individuabile un ulteriore *fil rouge* alla base degli interventi normativi di riforma, riconducibile all'esigenza di fronteggiare i rischi e le sfide relativi alla sicurezza delle transazioni, poste dalla circolazione dei dati[6].

Orbene, il fenomeno del c.d. *open banking*[7], che trova nella *access to account rule* uno degli elementi fondanti, sembra porre le basi per una

[3] Si tratta, peraltro, di servizi caratterizzati dalla circostanza che gli operatori che li offrono "non sono mai in possesso dei fondi del pagatore o del beneficiario" come precisato dalla Commissione europea nella Proposta di Direttiva COM (2013) 547 final 2013/0264,13.

[4] Per ragioni di concorrenza viene, infatti, imposta ai prestatori di servizi di radicamento dei conti di pagamento (tra cui le banche) una "collaborazione forzata" con i TPP. Cfr. B. Szego, "I nuovi prestatori autorizzati", in M.C. Paglietti, M.I. Vangelisti (a cura di), *Innovazione e regole nei pagamenti digitali*, cit., p. 166.

[5] La risoluzione in materia di FinTech del Parlamento europeo del 17.05.2017 (2016/2243/(INI)) afferma che "legislation and supervision in the area of FinTech should be based on the following principles: a) Same services and same risks: the same rules should apply, regardless of the type of legal entity concerned or its location in the Union; b) Technology neutrality; c) A risk-based approach, taking into account the proportionality of legislative and supervisory actions to risks and materiality of risks".

[6] L'esigenza di sicurezza dei pagamenti è ben evidenziata dai Considerando 95 e 96 della PSD2.

[7] Si tratta di quell'ecosistema avente la sua fonte nella PSD2 e caratterizzato dal diritto di accesso delle terze parti ai conti di pagamento detenuti dai propri clienti presso uno o più prestatori di servizio di radicamento del conto.

circolazione dei dati relativi ai conti di pagamento anche al di fuori delle ipotesi espressamente regolate dalla direttiva. Ciò potrebbe aprire un nuovo "mercato dei dati" per le banche e gli altri prestatori di servizi di radicamento dei conti (ASPSP – *Account Servicing Payment Service Providers*), che permetterebbe loro di sfruttare tale occasione commerciale con indubbi vantaggi, anche in ottica concorrenziale, per l'intero sistema dei pagamenti.

Occorre, però, verificare se la disciplina introdotta dalla PSD2 abbia effettivamente aperto il mercato alla (libera) commerciabilità del dato bancario, da parte delle banche *incumbents* in favore delle terze parti, permettendo così di qualificare tali dati come vere e proprie *digital commodities*[8]. Risulta, inoltre, necessario valutare se la disciplina sul trattamento dei dati personali di cui al Regolamento Generale sulla Protezione dei Dati 679/2016 (GDPR) costituisca un ostacolo alla libera circolazione dei dati bancari.

La soluzione a tali interrogativi impone l'analisi della disciplina dei nuovi servizi di pagamento introdotta dalla PSD2 e passa dalla risoluzione di talune questioni applicative, tanto di natura tecnica quanto giuridica, che saranno esaminate nel prosieguo.

2. *La PSD2 e i "nuovi" servizi di pagamento*

Come noto, la prima direttiva sui servizi di pagamento non ricomprendeva nel proprio ambito applicativo alcuni servizi innovativi di pagamento che si sono progressivamente imposti nella prassi commerciale, anche in ragione dell'evoluzione tecnica[9]. Ciò comportava che la prestazione

[8] Per gli aspetti definitori si veda *infra*, § 6.

[9] Si veda il Considerando n. 3 della Direttiva 2015/2366. Come osservato da V. Meli, *Opportunità e sfide per la concorrenza nella disciplina dei servizi di pagamento*, *in* M.C. Paglietti, M.I. Vangelisti (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento di interessi nella PSD2*, Roma, 2020, p. 155, la proposta di Direttiva 200764 era stata formulata nel 2005, quando ancora non era stato presentato al mercato il primo smartphone (strumento che successivamente sarebbe divenuto uno snodo fondamentale nei rapporti con la clientela e per l'operatività dei servizi di pagamento) e l'innovazione tecnologica non aveva raggiunto lo sviluppo odierno. Queste circostanze spiegano perché alcune forme di intermediazione – più strettamente legate all'innovazione tecnologica – non fossero contemplate dalla prima PSD2 Si deve, dunque, riconoscere il merito a tale disciplina di essere risultata sufficientemente elastica da adattarsi ad un mondo in continua evoluzione nonostante il *framework* normativo fosse pensato principalmente per un mondo (prevalentemente) analogico e non digitale.

di talune attività (tra cui la disposizione di ordini di pagamento o la raccolta di informazioni relative a conti di pagamento tenuti presso intermediari) fosse del tutto libera in quanto non soggetta ad autorizzazione né a specifici controlli sull'operatività. Tale assetto normativo determinava una situazione di incertezza e di vulnerabilità del sistema, nell'ambito del quale potevano operare soggetti non sottoposti agli stringenti controlli dell'autorità.

È proprio dall'esigenza di uniformità nella regolazione che muove la nuova disciplina che impone ai *Third Party Providers* di ottenere una *license* per poter offrire i servizi di *account information* e *payment initiation*, al pari dei tradizionali prestatori dei servizi di pagamento[10]. A tal riguardo, giova evidenziare che i PISP e AISP sono soggetti a condizioni – almeno teoricamente – meno gravose rispetto a quelle previste per gli istituti di pagamento e per gli istituti di moneta elettronica[11].

Questa diversa disciplina si giustifica alla luce dell'applicazione del principio di proporzionalità.[12] È, infatti, evidente che sottoporre questi operatori alle medesime regole previste per gli istituti di pagamento e IMEL (o addirittura quelle previste per le banche) avrebbe costituito una barriera all'entrata nel mercato e comunque sarebbe risultata ingiustificata attesa l'attività svolta in concreto dai TPP e i rischi connessi.

La circostanza che la disciplina applicabile a tali operatori sia effettivamente meno penetrante rispetto a quella prevista per gli istituti di pagamento, essendo i servizi offerti dai TPP radicalmente differenti e meno rischiosi per la stabilità del mercato, è però tutta da dimostrare: vi sono, infatti, numerosi indicatori[13] che portano a ritenere sproporzionati gli

[10] Cfr. art. 114 *sexies* e ss. del Testo Unico Bancario, D.lgs. 1 settembre 1993 n. 385.

[11] Con riferimento, ad esempio, ai requisiti di capitale minimo è previsto che i PISP debbano avere un capitale di almeno 50.000 euro (dunque, minore rispetto ai 125.000 euro di capitale minimo previsto per gli istituti di pagamento), mentre per gli AISP non è previsto alcun requisito minimo di capitale. Per i PISP e gli AISP è, inoltre, richiesto il possesso di una assicurazione per la responsabilità civile professionale.

[12] Sulla nozione di proporzionalità si vedano, tra gli altri, D.U. Galetta, *I principi di proporzionalità e ragionevolezza*, in M.A. Sandulli (a cura di), *Principi e regole dell'azione amministrativa*, Milano, 2015, pp. 69 ss.; A. Sandulli, *La proporzionalità dell'azione amministrativa*, Padova, 1998.

[13] Tra questi, si evidenzia che le Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica della Banca d'Italia del 23 luglio 2019 prevedono anche per i prestatori di servizi di informazione sui conti e di disposizione di pagamenti penetranti disposizioni relative ai requisiti degli amministratori: difatti, ai fini del rilascio dell'autorizzazione la Banca d'Italia è tenuta a verificare il "possesso da parte dei soggetti che svolgono funzioni di amministrazione, direzione e controllo nell'istituto di pagamento e nell'istituto di moneta elettronica dei requisiti di idoneità, previsti, rispettivamente, ai sensi dell'art. 114-novies, comma 1, lett. e-bis), e dell'art. 114-quinquies, comma 1,

strumenti regolatori applicati ai AISP e PISP[14].

A tal proposito, occorrerebbe valutare – in concreto, anche alla luce della disciplina secondaria applicata dalle autorità nazionali – se la minore incisività della regolazione dei TPP sia proporzionata rispetto alle attività da questi svolte o se, invece, non lo sia in quanto impiega categorie e strumenti propri della regolazione di soggetti che detengono denaro[15] e non adatti a coloro che operano solamente con i dati[16].

Ad ogni modo, la caratteristica più innovativa dei servizi di *account information service* è data dalla possibilità per i soggetti autorizzati al loro esercizio di operare sui conti di pagamento, tenuti dai propri clienti presso prestatori di servizi di radicamento di conti, a condizione che siano accessibili online[17].

---

lett. e-bis) del TUB". A ciò si aggiunga il complesso set documentale che le terze parti che intendano ottenere l'autorizzazione sono tenute a presentare, nell'ambito del quale deve essere fornita evidenza dell'adeguatezza delle misure di sicurezza adottate al fine di preservare l'integrità e la riservatezza dei dati.

[14] Anche nel *Final Report on the EBA Guidelines under Directive (EU) 2015/2366 (PSD2) on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers* sono chiaramente evidenziate le perplessità degli operatori economici con riferimento ad una eccessiva rigidità regolatoria nei confronti dei TPP. Giova, inoltre, evidenziarsi che i servizi di *account information* prima dell'entrata in vigore della PSD2 venivano considerati meri servizi informatici (ed erano soggetti, perciò, alla relativa disciplina).

[15] Difatti, anche l'art. 66 comma 3 lett. a) della PSD2, con riferimento ai servizi di disposizione di ordini di pagamento, precisa che i PISP non detengono in alcun momento i fondi del pagatore in relazione alla prestazione del servizio di disposizione di ordine di pagamento.

[16] Peraltro, sembrerebbe che l'approccio adottato dalle autorità nazionali nella verifica dei presupposti necessari per la concessione dell'autorizzazione e nella vigilanza delle terze parti non sia omogenea nell'ambito dell'UE. In tal modo, non è garantito il *level playing field*, essendo applicato un trattamento differenziato a operatori che svolgono la medesima attività, in considerazione del solo fatto che questi abbiano la propria sede principale in un determinato Paese membro. Ad esempio, nel Regno Unito e in Spagna si registra una minore rigidità dell'autorità di vigilanza e ciò emerge evidentemente anche dal maggiore numero di TPP *licensed* in tali Paesi.

[17] A ben vedere, la limitazione per cui tali servizi possono essere prestati solamente in relazione a conti correnti accessibili online è prevista espressamente dall'art. 4 comma 1 n. 16 con riferimento al solo servizio di informazione sui conti. Pur mancando una analoga previsione con riferimento ai servizi di disposizione di pagamento, si ritiene che tale limite sia contenuta nell'art. 22 della Direttiva 366/2015 che espressamente escluda il diritto per il pagatore di avvalersi del servizio di disposizione di pagamento allorquando il conto di pagamento non sia accessibile online. In tal senso, si veda V. Profeta, "I third party provider: profili soggettivi e oggettivi", in F. Maimeri e M. Mancini (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, Quaderni di Ricerca Giuridica della Consulenza Legale della Banca d'Italia, n. 87, settembre 2019, pp. 51 ss.

Similmente, anche i *payment initiation service providers* sono autorizzati ad accedere ai dati dei conti di pagamento.

In considerazione dell'essenzialità, per lo svolgimento dei servizi di *account information* e *payment initiation*, dell'accesso ai conti di pagamento tenuti dal cliente presso banche e prestatori di servizi di radicamento di conti di pagamento, il legislatore eurounitario ha, dunque, sancito l'obbligo per questi ultimi di consentire l'accesso ai conti, se autorizzati dal cliente e per le finalità previste dalla direttiva.

3. *L'accesso ai conti*

Una delle novità di maggiore rilievo della disciplina introdotta con la PSD2 – che rappresenta forte incentivo allo sviluppo dell'*open banking* – è proprio l'obbligo gravante sui prestatori di servizi di radicamento del conto di pagamento di permettere l'accesso ai dati relativi ai conti correnti[18]. In particolare, è riconosciuto ai *Third Party Providers* un diritto di accesso non oneroso e non rifiutabile (se non fornendo circostanziate motivazioni all'autorità competente) con specifico riferimento ai dati essenziali per la prestazione dei servizi di AISP e PISP.

Difatti, l'art. 36 della direttiva afferma che agli istituti di pagamento deve essere garantito in maniera obiettiva, proporzionata e non discriminatoria un accesso ai servizi relativi ai conti di pagamento degli enti creditizi. E tale accesso deve essere "*sufficientemente ampio da consentire all'istituto di pagamento di fornire servizi di pagamento in modo agevole ed efficiente*".

Tale previsione normativa – che non traccia in modo chiaro quali siano i dati che devono essere condivisi gratuitamente dalle banche né tantomeno quelli che (eventualmente) possano essere ceduti dietro corrispettivo – è rivolta anzitutto ai legislatori nazionali, che sono, dunque, chiamati a prevedere una *access to account rule* che sia "obiettiva, proporzionata e non discriminatoria".

E quindi, l'effettivo assetto della regola di accesso ai conti di pagamento dipende anche dalla disciplina nazionale di attuazione della direttiva[19].

[18] Occorre precisare che, sia nell'ambito della direttiva sia nella disciplina nazionale di recepimento, la "*access to account rule*" (*XS2A rule*) è declinata – con talune differenze – con riferimento a ciascuna tipologia di servizio di pagamento che può essere svolto da parte dei *Third Party Providers*.

[19] Peraltro, la norma europea non pone direttamente alcun vincolo di gratuità dell'accesso ai conti, ma si limita a fissare le condizioni di cui sopra che – in ipotesi – potrebbero

La disciplina italiana di recepimento, regolando l'accesso ai conti di pagamento di AISP e PISP, prevede che la prestazione del servizio "non è subordinata all'esistenza di un rapporto contrattuale tra il prestatore di servizi di disposizione di ordine di pagamento e il prestatore di servizi di pagamento di radicamento del conto";[20] la circostanza che non sia necessaria una previa relazione contrattuale tra la terza parte e il prestatore di servizi di pagamento di radicamento del conto avvalora, nell'ordinamento nazionale, la tesi della gratuità dell'accesso, atteso che manca la previsione di prezzi uniformi per l'accesso all'infrastruttura. Ad ogni modo, anche nell'ipotesi in cui il prestatore dei servizi di radicamento del conto ponesse a carico del proprio cliente l'eventuale prezzo per l'accesso dei TPP ai conti di pagamento ed il cliente poi non lo pagasse, il prestatore dei servizi di radicamento del conto non potrebbe comunque rifiutare l'accesso al conto alla terza parte.

Orbene, pur essendo l'imposizione della gratuità del diritto di accesso ai conti una misura di regolazione asimmetrica, che risulta giustificata in quanto finalizzata all'apertura del mercato con finalità pro-concorrenziali, si pone l'esigenza di comprendere chi siano i soggetti sui quali, di fatto, sono allocati i costi di questi servizi.

In tale contesto, vi è infatti il rischio che le banche siano tenute ad effettuare ingenti investimenti di adeguamento tecnologico, dovendosi conformare ai requisiti imposti dalla direttiva, e siano poi obbligate a cedere gratuitamente informazioni relative ai propri clienti, fondamentali per lo svolgimento del *business*. È, dunque, fondato il timore che, nell'ambito del settore dei servizi di pagamento, i c.d. soggetti *over the top* si possano collocare in un punto della catena del valore più remunerativa, mentre le banche potrebbero rimanere legate alle operazioni di deposito e alle strutture fisiche, più costose e meno remunerative (divenendo così delle *dumb pipes*[21], mere strutture di deposito). A parziale riequilibrio di tale assetto, occorre evidenziarsi che è opinione diffusa che le banche possano vendere alle terze parti le informazioni non rientranti nel novero di dati la

essere rispettate anche dalla previsione di un accesso sostanzialmente oneroso: infatti, il "prezzo" per permettere a soggetti terzi di accedere ai conti di pagamento ben potrebbe essere posto a carico del cliente, nell'ambito del canone annuale pagato alla banca (tra i costi di gestione del rapporto). Un siffatto assetto negoziale garantirebbe comunque il rispetto delle disposizioni poste dalla direttiva e sarebbe parimenti idoneo al raggiungimento delle finalità da questa perseguite.

[20] Art. 5 *ter* comma 1 del D.lgs. 27 gennaio 2010, n. 11, come modificato dal come modificato dal D.lgs. 218/2017.

[21] O. Borgogno, G. Colangelo, *Data, Innovation and Competition in Finance: The Case of the Access to Account Rule*, EU Law Working Paper, n. 35, 2018, p. 6; S. Vezzoso, *Fintech, Access to Data, and the Role of Competition Policy*, in *Competition and innovation*, 2018, 7.

cui condivisione è obbligatoria e gratuita. A ben vedere, esse potrebbero beneficiare della propria posizione di *incumbent* del mercato, cedendo (o meglio, condividendo), verso corrispettivo, dette informazioni ai nuovi operatori del settore dei servizi di pagamento[22].

Risulta, poi, necessario analizzare due ulteriori profili della *access to account rule*: quale sia il perimetro di dati la cui condivisione è obbligatoria e quali siano le finalità per le quali le terze parti possono impiegare i dati così ottenuti.

Con riferimento al primo punto, l'art 67 della direttiva, relativo all'accesso alle informazioni sui conti di pagamento per la prestazione di servizi di informazione sui conti, chiarisce che il prestatore di servizi "accede soltanto alle informazioni sui conti di pagamento designati e sulle operazioni di pagamento a questi associati". Evidentemente, la norma non individua con precisione i dati a cui il prestatore di servizi può aver accesso, ma si limita a ribadire che questi non possa accedere a informazioni relative a conti diversi rispetto a quello su cui deve essere svolta l'operazione richiesta dal cliente.

Quanto, invece, agli utilizzi che i TPP possono fare dei dati bancari dei propri clienti così acquisiti, la direttiva afferma che il prestatore dei servizi "non usa, accede o conserva dati per fini diversi da quelli della prestazione del servizio di informazione sui conti esplicitamente richiesto dall'utente dei servizi di pagamento, conformemente alle norme sulla protezione dei dati"[23]. Ebbene, quest'ultima previsione, di fatto, limita anche l'oggetto dei dati accessibili, circoscrivendolo a quelle informazioni finalizzate al servizio richiesto dal cliente.

Un'ulteriore indicazione in tal senso è fornita dall'art. 5 *ter* del D.lgs. 1/2010, come modificato dal D.lgs. 218/2017, che impone ai PISP di non chiedere al pagatore dati diversi da quelli necessari per prestare il servizio di disposizione di ordine di pagamento.

Alla luce di tali disposizioni normative, gli AISP e i PISP possono

[22] Potrebbe, così, realizzarsi il c.d. modello di *Banking-as-a-Platform* (BaaP). Le banche avrebbero la possibilità diventare una piattaforma che fornisce strumenti automatizzati e servizi al mercato. Cfr. G. Parker, M. Van Alstyne, S. Choudary, *Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You*, New York, 2016, p. 71.

[23] L'art. 66, relativo all'accesso ai conti di pagamento per la prestazione di servizi di disposizione di ordine di pagamento contiene previsioni normative che, sebbene differentemente formulate, contengono una disciplina analoga a quella di cui all'art. 67. Difatti, viene precisato che il TPP "non chiede all'utente dei servizi di pagamento dati diversi da quelli necessari a prestare il servizio di disposizione di ordine di pagamento" e "non usa né conserva dati né vi accede per fini diversi dalla prestazione del servizio di disposizione di ordine di pagamento come esplicitamente richiesto dal pagatore".

utilizzare, archiviare e accedere ai dati del conto, anche quando ciò non sia strettamente necessario per la prestazione del servizio richiesto dal cliente, solamente qualora intendano utilizzarli per migliorare il servizio, anche calibrandolo sulle caratteristiche del consumatore[24]. È evidente che così le terze parti possono analizzare grandi quantità di dati, che siano in qualche modo funzionali all'operazione disposta dal cliente e al miglioramento dell'esperienza di pagamento.

Gli è invece preclusa, ai sensi della PSD2, la possibilità di accedere a tali dati con finalità ulteriori, che non siano in alcun modo collegate alla prestazione dei servizi di pagamento.

Quanto alla legittimazione all'accesso ai conti da parte dei TPP, come chiaramente evidenziato dagli articoli 66 e 67 della PSD2, questa è subordinata alla prestazione del consenso esplicito da parte del cliente[25]. che, nell'impostazione della PSD2, costituisce l'unico meccanismo volto ad assicurare la liceità del trattamento dei dati personali[26].

Va, a tal riguardo, segnalato un *vulnus* di tutela per il cliente: il prestatore dei servizi di radicamento del conto non è tenuto ad effettuare controlli circa l'effettiva prestazione di tale consenso da parte del cliente potendo fare esclusivo andamento sul comportamento della terza parte che operi sul conto[27]. La ragione di siffatta compressione di tutela potrebbe individuarsi nelle tempistiche necessarie per svolgere i predetti controlli, di certo incompatibili con la rapidità dell'esecuzione dei pagamenti. Il cliente potrà comunque revocare in ogni momento il consenso all'accesso al proprio conto di pagamento da parte dei prestatori di servizi di informazione sui conti e di disposizione di ordini di pagamento, essendogli però preclusa la possibilità di revocare l'ordine di pagamento dopo aver prestato il proprio consenso all'operazione (salvo che vi ciò sia concordato dal cliente con tutti i prestatori di servizi coinvolti). La revoca del consenso prestato determinerebbe l'obbligo per i TPP di cancellare ogni dato del cliente in proprio possesso, senza più svolgere ulteriori attività che comportino l'utilizzo di tali dati, incluse quelle di analisi: come noto,

[24] Cfr. F. Di Porto, G. Ghidini, *'I Access Your Data, You Access Mine'. Requiring Data Reciprocity in Payment Services*, in *IIC – International Review of Intellectual Property and Competition Law*, 2020, 51, p. 318.

[25] È stato evidenziato da Profeta, *I third party provider*, cit., p. 71 che le modalità di prestazione del consenso per l'esecuzione delle singole operazioni – che ben potrà avvenire con strumenti informatici – potranno essere definite nell'ambito del contratto quadro sottoscritto dal TPP con il cliente.

[26] Cfr. *infra*, § 2.

[27] A mitigare il rischio derivante da tale situazione contribuisce certamente la circostanza che anche i *Third Party Providers* sono soggetti vigilati, tenuti ad obblighi di correttezza e sottoposti ad una rigida disciplina.

infatti, il consenso legittima il trattamento dei dati[28]. per le sole finalità correlate alla prestazione del servizio richiesto.

A ben vedere, la revoca del consenso alla prestazione dei servizi di *account information* e *payment initiation* determinerebbe automaticamente anche la revoca del consenso all'accesso ai propri dati bancari, quantomeno con riferimento a quelli il cui accesso era funzionale all'esecuzione di tale servizio.

A conferma di ciò, l'art. 6 *bis* del D.lgs. 11/2010 prevede, tra le cause legittimanti il rifiuto da parte del prestatore dei servizi di radicamento del conto dell'accesso al conto del TPP, la circostanza che il cliente abbia revocato il proprio consenso.

La rilevanza pratica della disciplina applicabile alla prestazione del consenso (e all'eventuale revoca del consenso) all'utilizzo di dati bancari assume maggiore rilevanza in ragione del valore economico che questi dati possono assumere e si inserisce nel più ampio dibattito sulla possibilità, e sulle eventuali modalità, con le quali il cliente possa opporsi allo sfruttamento commerciale dei propri dati da parte dell'istituto bancario presso cui è incardinato il conto di pagamento[29]. Si tratta di una questione indubbiamente centrale nell'ambito dell'analisi delle opportunità offerte dal nuovo assetto normativo della disciplina dei servizi di pagamento e del c.d. *open banking*, la cui soluzione passa necessariamente dal bilanciamento tra esigenze di circolazione e quelle di tutela dei dati personali[30].

[28] Per trattamento dei dati personali, ai sensi dell'art. 4, comma 1, n. 2) GDPR si intende "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il affronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

[29] Il GDPR disciplina espressamente alcuni strumenti con i quali il soggetto interessato al trattamento dei dati può limitare l'uso che possa farne il responsabile del trattamento: ai sensi dell'art. 18 il soggetto interessato al trattamento dei dati ha diritto alla limitazione del trattamento qualora questo possa essergli pregiudizievole; l'art. 21, invece, prevede il diritto dell'interessato di opporsi "per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni", imponendo così al titolare del trattamento di astenersi dal trattare ulteriormente i dati. D'altra parte, l'art. 7 comma 3 riconosce all'interessato il diritto di revocare – in ogni momento – il consenso al trattamento dei dati, precisando che "la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca". Si veda sul punto G. Di Lorenzo, *Spunti di riflessione su taluni 'diritti dell'interessato'*, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, pp. 248 ss.

[30] I dati personali sono definiti dall'art. 4, comma 1, n. 1) del GDPR come "qualsiasi infor-

Certamente, la disciplina sul diritto di acceso dei TPP ai conti – di cui all'art. 36 della direttiva – apre (o quantomeno ha tutte le potenzialità per aprire) nuove opportunità di sviluppo, in quanto impone alle banche di implementare le tecnologie occorrenti per la condivisione dei dati rendendo, così, i conti di pagamento delle vere e proprie infrastrutture la cui piena (ed efficiente) operatività ed accessibilità è necessaria al fine di consentire la concorrenza. Non viene chiarito, però, se (ed eventualmente, a quali condizioni) le banche possano sfruttare le opportunità derivanti dall'obbligo di predisposizione delle interfacce di collegamento al fine di cedere – a fronte di un corrispettivo – alle terze parti dati ulteriori (relative ai medesimi clienti) rispetto a quelli la cui condivisione è obbligatoria. Non è neppure precisato se possano cedere – anche in massa – dati bancari relativi a propri clienti, pur in mancanza di una relazione contrattuale tra il TPP "acquirente" e i clienti della banca i cui dati sono ceduti. Su tali profili ci si soffermerà *infra*, § 6.

Ad ogni buon conto, giova evidenziare che la possibilità per i prestatori dei servizi di radicamento dei conti di valorizzare e commerciare i dati in proprio possesso non solo non è espressamente esclusa dalla direttiva, ma anzi appare in linea con le finalità pro-competitive perseguite dal legislatore europeo con l'intervento di riforma. D'altra parte, però, con l'introduzione della regola dell'*access to account* è stato riconosciuto al cliente, soggetto interessato al trattamento dei dati, il potere di consentirne l'utilizzo a terzi, sebbene con riferimento alle sole finalità delineate dalla direttiva[31], limitando così il potere sui dati spettante alla banca che aveva raccolto tali informazioni nell'ambito della propria attività.

Il titolare del conto di pagamento ha, dunque, diritto di accedere ai dati del conto di pagamento, anche avvalendosi dei servizi offerti dai *Third Party Providers*, che operano per suo conto:[32] l'art. 67 PSD2, infatti, prevede che il diritto di ricorrere a servizi che richiedono l'accesso al conto debba essere riconosciuto al titolare del conto e solo mediatamente alle terze parti (che agiscono, appunto, per conto del titolare del conto). Come detto, questo

mazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

[31] Gli articoli 66 e 67 della PSD2 prevedono, infatti, che sia il cliente a decidere se e quando i propri dati personali, detenuti dalla banca o dal prestatore di servizi di radicamento del conto di pagamento, debbano essere condivisi con AISP e PISP.

[32] Burchi, Mezzacapo, Musile Tanzi, Troiano, *Financial Data Aggregation*, cit., pp. 25 ss.

nuovo approccio al trattamento dei dati (personali) del cliente adottato dalla PSD2 pone, però, esigenze di coordinamento con la disciplina generale sul trattamento dei dati personali di cui al Regolamento UE 679/2016 (GDPR)[33].

Difatti, la PSD2 si limita a disciplinare gli aspetti relativi alla prestazione del consenso, da parte del cliente, finalizzato a consentire alle terze parti l'accesso ai dati, per la finalità correlate alla prestazione dei servizi di *account information* e *payment initiation*, ma nulla dice con riferimento a possibili ulteriori impieghi dei dati (che non siano in alcun modo collegati con la prestazione del servizio richiesto dal cliente). Tali utilizzi potrebbero ritenersi esclusi, proprio perché la direttiva precisa che il TPP non possa utilizzare, accedere o conservare i dati per finalità diverse da quelle della prestazione del servizio richiesto.

Rimane, però, da verificare se il trattamento di ulteriori dati personali del cliente sia legittimo qualora il cliente vi acconsenta o se, invece, l'eventuale cessione di tali dati si ponga in contrasto con la disciplina del GDPR. Sul punto si tornerà nei paragrafi successivi.

La condivisione (ed eventuale compravendita) dei dati relativi ai clienti deve, in ogni caso, avvenire mediante strumenti tecnici adeguati, idonei a garantire la sicurezza e la riservatezza delle informazioni veicolate. A tal proposito, la direttiva e i *Regulatory Technical Standards* adottati dalla Commissione europea su proposta dell'EBA fissano il contenuto minimo dei protocolli di comunicazione tra prestatori di servizi di radicamento dei conti di pagamento e terze parti, le c.d. *Application Programming Interfaces* (API)[34], con la finalità precipua di garantire la sicurezza delle operazioni (oltre a garantire una minima omogeneità degli strumenti tecnici impiegati).

[33] Sul punto V. Zeno-Zencovich, *Prefazione*, in M.C. Paglietti, M.I. Vangelisti (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento di interessi nella PSD2*, Roma, 2020, pp. 10 ss. L'autore evidenzia come l'impostazione della PSD2 "collide frontalmente con la retorica della protezione dei dati personali, incarnata dal Regolamento generale sulla protezione dei dati personali" mettendo in luce "la elefantiaca declamatorietà del GDPR". Alcuni chiarimenti circa il coordinamento tra GDPR e PSD2 sono stati forniti dallo *European Data Protection Board* (EPDB) al Parlamento europeo con lettera del 1 luglio 2018.

[34] Articoli 30 e seguenti del Regolamento delegato (UE) 2018/389 della Commissione europea del 27 novembre 2017 che reca le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri.

4. *Le* Application Programming Interfaces

Le *Application Programming Interfaces* costituiscono interfacce di collegamento e comunicazione tra diversi soggetti, che permettono lo scambio di dati e informazioni[35]. Nell'ambito dell'ecosistema Fintech, le API costituiscono il principale strumento tecnico per consentire l'accesso dei *Third Party Providers* ai conti di pagamento di cui i propri clienti siano titolari presso uno o più istituti di radicamento dei conti. Si tratta, perciò, di sistemi di accesso ai dati conservati presso *database* o *server*,[36] finalizzati alla cooperazione tra due o più soggetti.

Orbene, con riferimento alle modalità di accesso dei TPP ai conti di pagamento, la direttiva prevede che gli AISPS predispongano interfacce di collegamento dedicate che abbiano livelli di disponibilità e prestazioni non inferiori rispetto alle interfacce a disposizione del cliente per l'accesso diretto al proprio conto online. Alternativamente, come evidenziato dal Considerando n. 32 della PSD2, i prestatori di servizi di radicamento del conto possono garantire alle terze parti un accesso "indiretto" ai conti di pagamento, utilizzando le medesime interfacce a disposizione del cliente per l'accesso al proprio conto *online*.

L'art. 33 degli RTS disciplina, poi, le misure di emergenza per le interfacce dedicate, volte a porre rimedio a possibili indisponibilità o malfunzionamenti delle API. Si tratta della c.d. *fallback solution* in base alla quale i prestatori di servizi di radicamento dei conti sono tenuti a prevedere modalità alternative di accesso, tra cui la messa a disposizione di

[35] Si tratta di un insieme di definizioni e protocolli volti ad integrare l'operatività di diversi programmi. Più nello specifico, le API costituiscono applicazioni che, mediante modalità standardizzate, rendono accessibili le informazioni e le funzionalità di altre applicazioni. Sono state definite da J. Stylos, A. Faulring, Z. Yang, B.A. Myers, *Improving API documentation using API usage information*, in *Proceedings of IEEE Symposium on Visual Languages and Human-Centric Computing*, Washington, 2009, pp. 119 ss. come quello strumento volto a "expose services or data provided by a software application through a set of predefined resources, such as methods, objects or URIs".

[36] Cfr. O. Borgogno, *Regimi di condivisione dei dati ed interoperabilità: il ruolo e la disciplina delle A.P.I.*, in *Diritto dell'informazione e dell'informatica*, 3, 2019, p. 689. L'autore evidenzia che le API possono avere diversi livelli di complessità, in quanto possono essere dei semplici collegamenti a *database* o *dataset* o, invece, collegamenti a delle interfacce online. Occorre, inoltre, precisare che le *Application Programming Interfaces* debbono essere suddivise in API interne ed API esterne: se le prime sono quelle funzionali alla circolazione dei dati nei processi interni ad una singola impresa, le API esterne (come quelle la cui predisposizione è imposta dalla disciplina della PSD2) "permettono l'integrazione con soggetti terzi (collaboratori, sviluppatori esterni o, anche, imprese concorrenti) facilitando l'accesso a specifici dataset, nonché lo sviluppo di nuove e migliori tecniche di cooperazione".

un meccanismo in base al quale i TPP possano accedere alle interfacce per l'accesso dei clienti.

In ragione della gravosità dell'obbligo di predisporre – di fatto – due meccanismi alternativi di comunicazione tra istituti di radicamento del conto e TPP, gli stessi RTS hanno stabilito che le autorità nazionali possano esonerare gli istituti di radicamento di conti dal predisporre una *fallback solution* allorquando l'interfaccia dedicata affra sufficienti requisiti di sicurezza e affidabilità[37]. Tale soluzione è volta a contemperare le esigenze di sicurezza e continuità del funzionamento dell'interfaccia di collegamento e la necessità di evitare l'imposizione di obblighi che siano eccessivamente gravosi per gli AISPS.

È proprio in considerazione dell'esigenza di rispettare standard minimi di sicurezza delle operazioni che la direttiva ha limitato il ricorso alla pratica (assai diffusa prima dell'entrata in vigore della PSD2) del c.d. *screen scraping* in base alla quale ai prestatori di servizi di pagamento non era dedicata un'apposita interfaccia per l'accesso ai conti di pagamento, bensì questi vi accedevano utilizzando le credenziali dello stesso cliente[38]. Ne derivavano gravi problemi di sicurezza, poiché non era univocamente individuabile il soggetto che aveva operato sul conto (mancando una chiave di acceso univoca per i TPP), con le immaginabili conseguenze sulla prova della responsabilità del prestatore del servizio.

Alle banche e ai prestatori di sevizi di radicamento dei conti di pagamento accessibili *online* viene, dunque, imposto (pur con le eccezioni menzionate) l'obbligo di predisporre interfacce digitali di collegamento con le terze parti, che siano idonee dal punto di vista della sicurezza e dell'accessibilità e che permettano agli operatori del settore di scambiare informazioni relative ai servizi di pagamento[39].

[37] Cfr. art. 33 comma 6 RTS. Con nota del 4.01.2019, la Banca d'Italia ha indicato le condizioni per beneficiare dell'esenzione dall'obbligo di predisposizione della *fallback solution*.

[38] Il TPP, in questo modo, non solo svolgeva l'attività per conto del cliente ma – di fatto – anche in nome di questi, eseguendo direttamente la prestazione richiesta e operando sul conto di pagamento con le credenziali del cliente. Ad oggi, invece, l'accesso da parte dei TPP ai conti di pagamento deve avvenire necessariamente in modo "formale", senza che questi possano rimanere anonimi.

[39] Il Considerando n. 20 Regolamento delegato (UE) 2018/389 della Commissione europea del 27 novembre 2017 afferma che "Tutti i prestatori di servizi di pagamento di radicamento del conto con conti di pagamento accessibili online dovrebbero offrire almeno un'interfaccia di accesso che consenta la comunicazione sicura con i prestatori di servizi di informazione sui conti, i prestatori di servizi di disposizione di ordine di pagamento e i prestatori di servizi di pagamento che emettono strumenti di pagamento

Si tratta di strumenti essenziali per la piena operatività dei servizi di *open banking*: dall'efficienza delle API dipende il corretto funzionamento dei processi e quindi risulta di particolare rilevanza la definizione delle caratteristiche di queste interfacce.

In applicazione del principio della neutralità tecnologica[40], il legislatore europeo non ha però definito normativamente le soluzioni tecniche da adottare con riferimento alle API, ma si è limitato a fissare alcuni prerequisiti necessari per garantire l'affidabilità e l'efficienza degli strumenti di pagamento[41]: ai sensi dell'art. 98 PSD2, la definizione della disciplina tecnica relativa a tali aspetti è affidata all'EBA, alla quale spetta la redazione dei *Regulatory Technical Standards*, approvati dalla Commissione europea.

In particolare, l'art. 30 dei RTS chiarisce che le interfacce di accesso devono essere basate su standard di comunicazione sicura e procedure di autenticazione forte[42], ribadendo così la centralità – nell'ambito dell'impianto della disciplina introdotta dalla direttiva – della sicurezza delle comunicazioni e dell'identificabilità del prestatore di servizio. L'implementazione delle API da parte delle banche permette, dunque, di accrescere i livelli di sicurezza nella condivisione dei dati.

Occorre però ribadire che l'adeguamento delle strutture delle banche e degli altri prestatori di servizi di radicamento dei conti alle caratteristiche tecniche minime imposte dalla direttiva e dagli RTS determina costi per gli

basati su carta".

[40] Si tratta di un principio cardine della disciplina, volto ad evitare distorsioni del mercato e ostacoli alla concorrenza. A tal riguardo, il Considerando n. 21 della Direttiva 2366/2015precisa che "la definizione dei servizi di pagamento dovrebbe essere neutra sotto il profilo tecnologico e consentire lo sviluppo di nuovi tipi di servizi di pagamento, garantendo pari condizioni operative ai prestatori di servizi di pagamento esistenti e ai nuovi prestatori". Il principio di neutralità tecnologica è, poi, confermato anche dal Considerando n. 20 dei *Regulatory Technical Standards* che non solo non individua una particolare tecnologia da impiegarsi per le interfacce, ma chiarisce che "Per assicurare la neutralità dal punto di vista tecnologico e del modello di attività, i prestatori di servizi di pagamento di radicamento del conto dovrebbero essere liberi di decidere se offrire un'interfaccia dedicata per la comunicazione con i prestatori di servizi […] se consentire, ai fini di tale comunicazione, l'uso dell'interfaccia per l'identificazione e la comunicazione con gli utenti dei servizi di pagamento dei prestatori di servizi di pagamento di radicamento del conto".

[41] D. Gammaldi, C. Iacomini, *Mutamenti nel mercato dopo la PSD2*, in F. Maimeri e M. Mancini (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, Quaderni di Ricerca Giuridica della Consulenza Legale della Banca d'Italia, n. 87, settembre 2019, p. 137.

[42] L'identificazione dei prestatori di servizi viene garantita mediante l'utilizzo di certificati digitali rilasciati dai *Quality Trust Service Providers* disciplinati dal Regolamento UE 910/2014.

operatori economici che potrebbero essere grandemente ridotti qualora le banche e gli altri soggetti interessati si coordinassero per la determinazione di standard comuni, pur non essendo questi fissati dalla legge.

È dibattuto se la decisione legislativa di non predeterminare le caratteristiche tecniche delle API sia idonea a garantire il *level playing field*. Difatti, la circostanza che non sia stata operata la scelta neppure di uno specifico linguaggio di programmazione di tali interfacce espone le terze parti al rischio di dover sostenere ingenti costi al fine di poter interagire con le API predisposte da ciascun intermediario e ciò potrebbe rappresentare una barriera all'ingresso (chiaramente confliggente con l'intento pro-concorrenziale della condivisione dei dati).

La scelta di non imporre per via normativa l'utilizzo di specifiche tecnologie o linguaggi di programmazione appare volta a mantenere un approccio neutrale circa l'individuazione della tecnologia utilizzabile in quanto non sembrerebbero esserci, ad oggi, strumenti di collegamento e condivisione dei dati tra i TPP e i prestatori di servizi di radicamento del conto di pagamento che garantiscano i medesimi livelli di sicurezza delle API[43]. Ciò nonostante, le critiche circa i possibili aggravi per i TPP dettati dalla possibilità che le banche predispongano API aventi caratteristiche tra loro difformi appare sicuramente fondata. Guardando, però, al fenomeno in chiave prospettica, la circostanza che sia lasciata al mercato la scelta circa l'individuazione degli strumenti tecnici più adeguati per operare da snodo tra intermediari bancari e terze parti potrà innescare un processo competitivo volto ad individuare le soluzioni più efficienti. Una siffatta efficienza dinamica non potrebbe realizzarsi, invece, qualora venisse imposto per legge un modello di interfaccia di collegamento.

Nel silenzio normativo, diverse sono state le impostazioni accolte. Se in Italia si è preferita una soluzione di mercato – la quale ha lasciato spazio agli operatori privati nella determinazione della soluzione tecnica più adatta – diversamente nel Regno Unito l'autorità amministrativa ha favorito l'elaborazione di un modello di API standardizzato[44].

[43] È stato evidenziato come, in futuro, una valida alternativa potrebbe essere fornita dall'utilizzo della tecnologia *blockchain*, purché le banche sostituiscano i *database* individuali con registri di informazioni condivise trasferibili tramite *blockchain*. In tal senso, A. Sciarrone Alibrandi, *Impostazione sistematica della Direttiva PSD2*, in M.C. Paglietti, M.I. Vangelisti (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento di interessi nella PSD2*, Roma, 2020, p. 21.

[44] Il tentativo dello *European Retail Payment Board* di favorire il raggiungimento di uno standard tecnico condiviso che fosse idoneo a soddisfare i requisiti tecnici non ha avuto esito positivo e i modelli di API elaborati da altri organismi privati non sono comunque vincolanti per gli operatori. Peculiare è l'esperienza inglese, dove la *Competition and*

Pur potendo avere le banche interesse – con approccio "protezionistico" – ad adottare API basate su tecnologie differenti tra loro, al fine di rendere più complesso (e costoso) l'adeguamento a tali molteplici tecnologie da parte dei TPP, occorre precisare che l'integrazione, nell'ambito del sistema dei pagamenti, di banche e operatori Fintech – a regime – potrebbe essere in grado di aumentare il giro d'affari complessivo del settore, con effetti benefici anche per le banche. È, dunque, chiaro che comportamenti ostruzionistici dei prestatori dei servizi di radicamento dei conti, volti ad evitare che si raggiunga uno standard efficiente di API, sul lungo periodo sarebbero controproducenti e lesivi per l'intero sistema.

Ebbene, sono anche le caratteristiche tecniche delle API e la diffusione di questi strumenti – derivante dalla necessità di adeguarsi agli obblighi normativi – a favorire lo sviluppo di una *data driven economy*.

5. *Compatibilità con il GDPR*

Il mercato dei dati costituisce un elemento fondamentale del mercato digitale[45] e, con questa consapevolezza, il legislatore eurounitario ha riconosciuto al soggetto che detenga tali dati il diritto di disporne, purché ciò avvenga nel rispetto delle condizioni di liceità del trattamento. Peraltro, il soggetto interessato a cui i dati personali si riferiscono conserva un interesse all'utilizzo delle informazioni raccolte dal responsabile del trattamento dei dati, parimenti tutelato dalla disciplina europea.

Proprio con tale finalità, l'art. 20 GDPR disciplina il diritto alla portabilità dei dati, in forza del quale il soggetto interessato ha diritto di ricevere copia dei dati personali che lo riguardano, che ha fornito al titolare del trattamento, e di trasmetterli ad altro titolare del trattamento. Da questo punto di vista, la *access to account rule* costituisce una regola speciale, in quanto settoriale, rispetto al più ampio diritto alla portabilità dei dati di cui

Markets Authority ha incaricato le otto banche principali del Paese di sviluppare congiuntamente un modello aperto e standardizzato di API, poi elaborato da *Open Banking UK*, al fine di promuovere la condivisione di dati tra banche e terze parti. In Italia, invece, sono state predisposte una pluralità di soluzioni di mercato: si segnalano, tra le altre, le proposte tecniche elaborate da CBI Globe, Cedacri e Fabrick.

[45] Cfr. Comunicazione della Commissione europea del 10.01.2017 [COM (2017) 9 final] volta a costruire un'economia dei dati europei e la Comunicazione del 25.04.2018 [COM (2018) 125 final] sullo spazio europeo dei dati.

al GDPR.[46] L'idea di fondo, comune alle due discipline (quella settoriale e quella generale) è riconducibile all'intenzione di perseguire una maggiore contendibilità dei dati personali detenuti dagli operatori tradizionali presenti sul mercato, attribuendo al soggetto interessato il potere di chiedere al responsabile del trattamento dei dati di trasferirli ad un altro soggetto.[47]

La regola di cui all'art. 36 della PSD2, permettendo al soggetto interessato al trattamento dei dati di disporre dei propri dati detenuti da un prestatore di servizi di radicamento del conto e consentendo ad un altro operatore economico di accedervi, sembra non aggiungere molto alla regola generale contenuta nel GDPR[48].

Quel che occorre indagare è se – anche al di fuori delle ipotesi disciplinate agli articoli 36, 66 e 67 PSD2 – i dati relativi ai conti di pagamento possano essere ceduti dal titolare del trattamento (prestatore del servizio di radicamento del conto) ad altri soggetti e, in tal caso, a quali condizioni ciò possa avvenire. In altri termini, deve valutarsi se i dati relativi ai conti di pagamento possano essere considerati alla stregua di beni commerciabili e se possano cioè essere ceduti a titolo oneroso a soggetti terzi, anche qualora questi ultimi non intrattengano alcun rapporto con il cliente – interessato al trattamento dei dati personali.

A fini di chiarezza espositiva, risulta utile enumerare le ipotesi di cessione di tali dati che il prestatore di servizi di radicamento del conto di pagamento (responsabile del trattamento dei dati) potrebbe in astratto realizzare.

Accanto alla cessione dei dati necessari alla prestazione dei servizi di *account information* e *payment initiation*, la cui condivisione è contemplata dalla direttiva, il prestatore di servizi di radicamento del conto di pagamento avrebbe interesse a cedere a titolo oneroso, alle stesse terze parti alle quali ha ceduto i dati necessari alla prestazione dei servizi richiesti dal cliente, ulteriori dati relativi al medesimo utente.

Vi sono poi almeno due ulteriori assetti negoziali da valutare: la cessione di dati di pagamento relativi ad un singolo cliente, che non abbia però

[46] I. Graef, M. Husovec, N. Purtova, *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*, in *German Law Journal*, 2018, 19, 6, pp. 1359 ss.

[47] Anche nell'ambito delle ipotesi disciplinate dal GDPR, la portabilità dei dati è subordinata all'esistenza di una interfaccia di collegamento tra il responsabile del trattamento dei dati personali e il soggetto a favore del quale è richiesto il trasferimento. In mancanza di una infrastruttura di questo tipo – che può essere strutturata come una API – vi sono ostacoli tecnici alla realizzazione della portabilità dei dati.

[48] Sebbene vi sia un rapporto di genere a specie tra le due discipline, giova sottolinearsi che le disposizioni contenute nella PSD2 sono cronologicamente precedenti rispetto a quelle del Regolamento 679/2016.

alcun rapporto con l'acquirente dei dati, nonché la cessione in blocco di dati (anonimizzati[49] o meno) dei clienti del prestatore di servizi di radicamento del conto a soggetti terzi.

In mancanza di una disposizione normativa che espressamente regoli tali ipotesi, per dare risposta al quesito circa la libera commerciabilità dei dati bancari, è opportuno effettuare alcune riflessioni, analizzando la disciplina del GDPR e ponendola a confronto con quella recata dalla PSD2[50].

Ebbene, nell'ambito del c.d. modello informazionale della realtà[51], che si è imposto grazie alla diffusione delle nuove tecnologie, la libera circolazione delle informazioni è una condizione normale,[52] la quale può essere limitata solamente a fronte di esigenze prevalenti.

Proprio grazie a questa concezione dei dati come beni[53] naturalmente destinati a circolare (e che possono, perciò, essere oggetto di contratti) si coglie lo scopo perseguito dal legislatore con la PSD2. La finalità di apertura del mercato dei servizi di pagamento a nuove iniziative imprenditoriali passa anche per la cedibilità dei dati bancari, pure al di fuori delle ipotesi in cui ciò è imposto obbligatoriamente dalla legge.

Orbene, la regola generale impone, per le operazioni con le quali si realizzi l'accesso ai dati (compresa la cessione a terzi) l'espressa prestazione del consenso del cliente quale condizione di liceità. L'art. 6 del GDPR, al fine di garantire maggiore efficienza dell'utilizzo dei dati personali, prevede anche condizioni di liceità del trattamento ulteriori e alternative al consenso

[49] Il Considerando n. 26 al GDPR evidenzia: "I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca".

[50] Preliminarmente, risulta utile evidenziare che l'ambito soggettivo di applicazione delle due discipline non è coincidente: difatti, mentre il GDPR "stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati" (art. - GDPR), l'art. 94 della PSD2 non prevede simili limitazioni e sembra, dunque, doversi applicare anche al trattamento dei dati non riconducibili a persone fisiche.

[51] In tale modello, le nuove tecnologie non sarebbero meri strumenti di comunicazione, quanto piuttosto determinerebbero una vera e propria "riconcettualizzazione delle categorie". In tal senso L. Floridi, *Infosfera. Etica e filosofia nell'età dell'informazione*, Torino, 2009, p. 185.

[52] R. Messinetti, *Circolazione dei dati personali e autonomia privata*, *Federalismi.it*, 21, 2019.

[53] V. Zeno-Zencovich, *Cosa*, in *Digesto delle discipline privatistiche. Sezione civile*, IV, Torino, 1989, p. 453.

del soggetto interessato.

La previsione di condizioni di liceità del trattamento dei dati alternative al consenso, di cui all'art. 6 GDPR, volte a semplificare l'utilizzo e il trattamento dei dati, mette in luce l'esistenza di una tensione tra l'istanza circolatoria e l'esigenza di tutela della privacy[54], che si frappone ad un pieno diritto alla commerciabilità dei dati.

Nell'ambito di tale sistema, al consenso del soggetto interessato al trattamento dei dati è, dunque, riconosciuto il ruolo di regola di governo della cedibilità dei dati stessi, purché non ricorrano le altre ipotesi di cui all'art. 6 del Regolamento[55].

Occorre, dunque, valutare quali tra le condizioni di liceità del trattamento di cui all'art. 2 GDPR possano venire in rilievo con riferimento alla cessione a terzi dei dati relativi ai conti di pagamento.

Quanto alle condizioni di liceità del trattamento diverse dal consenso, la cessione di dati bancari da parte dei prestatori di servizio di radicamento di conti di pagamento in favore di terze parti non sembra possa essere ricondotto all'ipotesi di cui all'art. 6 comma 1 lett. b) del GDPR, secondo cui il trattamento è lecito se sia necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.

Difatti, nelle ipotesi di cessione dei dati bancari di cui ci si sta occupando (al di fuori di quelle espressamente regolate dagli articoli 66 e 67 PSD2) non vi sarebbe alcun contratto da eseguirsi di cui il titolare del conto di pagamento (interessato al trattamento dei dati) sia parte[56]. E dunque, occorre individuare una diversa base giuridica che consenta tale operazione di trattamento dei dati, atteso comunque il *favor* normativo rispetto ai fenomeni circolatori dei dati.

---

[54] D. Messinetti, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, pp. 339 ss.

[55] È stato, a tal proposito, messo in evidenza in R. Messinetti, *Circolazione dei dati personali e autonomia privata*, cit., p. 11 che "la residualità del consenso rinvia al carattere non assoluto che il diritto fondamentale della persona all'autodeterminazione informativa riveste nel sistema del diritto europeo; cioè alla sua bilanciabilità con altri principi fondamentali". Sulla configurabilità delle condizioni di liceità consenso quali meccanismi di selezione dei degli interessi tutelati si veda F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018, p. 61.

[56] Al contrario, con riferimento alla ipotesi in cui sia il titolare del conto di pagamento a richiedere che i dati siano condivisi al fine di ottenere i servizi di *account information* o *payment initiation*, il trattamento dei dati è finalizzato all'esecuzione di un contratto. In tal caso, però, la base giuridica di tale trattamento si individua nella *lex specialis* degli artt. 66 e 67 della PSD2.

L'art. 6 comma 1 lett. f) del GDPR prevede un'ulteriore condizione di liceità del trattamento dei dati che potrebbe venire in rilievo nel caso di specie: quando sia "necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore".

Si tratta di una norma con contenuto indeterminato, che risponde alla necessità di tutelare le istanze circolatorie[57] e legittima il trattamento dei dati personali pur in mancanza di un espresso consenso del soggetto interessato.

Resta, però, da chiarire cosa si debba intendere per legittimo interesse del titolare del trattamento o dei terzi, al fine di valutare se l'ipotesi di compravendita di dati bancari possa ritenervisi ricompresa. È, difatti, evidente che maggiore è l'ambito applicativo che viene riconosciuto alla nozione di legittimo interesse quale condizione di liceità del trattamento dei dati personali, minore è lo spazio riservato al consenso quale strumento mediante il quale il soggetto interessato al trattamento dei dati può decidere se intenda permettere o meno il trattamento dei propri dati da parte di un terzo[58].

Quella del legittimo interesse è una nozione evanescente, che non è definita espressamente dal Regolamento, il quale però dedica ben quattro Considerando all'individuazione di ipotesi che vi rientrano. A tal riguardo, il Considerando n. 47 precisa che "l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine". Il Considerando n. 50 chiarisce, invece, che "Il trattamento dei dati personali per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti dovrebbe essere consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti. In tal caso non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati personali".

Ciò non permette di ritenere univocamente utilizzabile la condizione di

[57] Come evidenziato da D. De Paoli, *PSD2 e privacy*, in M.C. Paglietti, M.I. Vangelisti (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento di interessi nella PSD2*, Roma, 2020, p. 147 il consenso privacy – che è cosa differente dal consenso contrattuale – non è necessario in quelle situazioni nelle quali sono in gioco dati che possono essere trattati dai titolari del trattamento sulla base della clausola del legittimo interesse del titolare del trattamento.

[58] D. Baldini, *Il difficile equilibrio tra consenso della persona interessata e legittimo interesse del titolare del trattamento: problemi e prospettive nei rapporti tra fonti interne e dell'Unione europea in tema di tutela dei dati personali*, in *Osservatorio sulle fonti*, 3, 2017, p. 2.

liceità di cui all'art. 6 comma 1 lett. f) GDPR quale base giuridica per la cessione dei dati bancari a terzi, pur agendo il titolare del trattamento dei dati in attuazione del proprio diritto costituzionalmente tutelato (41 Cost.) di libera iniziativa economica.

Peraltro, anche il parere dell'art. 29 WP, reso con riferimento alla disciplina previgente al GDPR, ha elaborato un'ampia casistica di ipotesi rientranti nell'ambito applicativo del "legittimo interesse" tra cui non rientra lo sfruttamento commerciale mediante cessione a terzi a titolo oneroso di dati personali dei propri clienti[59].

È dunque, l'applicabilità della condizione di liceità del trattamento dei dati personali di cui all'art. 6 comma 1 lett. f) GDPR, pur essendo pienamente in linea con le finalità di sviluppo dell'economia digitale perseguite dal legislatore eurounitario[60], non sembra appropriata al caso di specie.

Alla luce di ciò, pur non essendo sufficiente l'esistenza di un interesse commerciale del responsabile del trattamento, sembrerebbe ad ogni modo che non vi siano ostacoli alla commerciabilità dei dati bancari da parte dei prestatori di servizio di radicamento di conti di pagamento in favore di terze parti, purché il soggetto interessato al trattamento dei dati abbia prestato il consenso al trattamento dei propri dati ai sensi dell'art. 6 comma 1 lett. a) GDPR, con specifico riferimento alle finalità di sfruttamento commerciale.

Occorre, però, verificare se la disciplina del GDPR sia compatibile con il peculiare trattamento riservato ai dati bancari nell'ambito della regolazione dei servizi di pagamento o se, in ragione della specialità di quest'ultima, vi siano ostacoli alla cessione a titolo oneroso dei dati bancari dei clienti a terze parti.

A tal proposito, deve rilevarsi che l'art. 29, comma 1 bis del D.lgs. 11/2010 prevede che i prestatori di servizi di pagamento "hanno accesso, trattano e conservano i dati personali necessari alla prestazione dei rispettivi servizi di pagamento, solo previo consenso esplicito dell'utente"[61]. Si tratta

[59] Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, adottato il 9 aprile 2014, 844/14/EN WP 217, pp. 23 ss.

[60] Viene così favorita la c.d. capacità immaginativa dell'autonomia contrattuale, che è volta a creare nuove forme di ricchezza, anche impiegando nuovi schemi contrattuali. Cfr. F. Galgano, *Lex mercatoria*, Bologna, 2010, pp. 239 ss. Il commercio dei dati bancari ha certamente la potenzialità per aprire nuovi mercati – creando nuova ricchezza – attraverso la valorizzazione dei dati raccolti dalle banche e dagli altri prestatori di servizi di radicamento del conto.

[61] Comma introdotto dal D.lgs. 218/2017.

di una regola avente portata generale nell'ambito della disciplina dei servizi di pagamento, che sembra derogare al regime posto dall'art. 2 GDPR, in ragione del principio di specialità. È stato precisato che il consenso a cui fa riferimento l'art. 29 (in trasposizione di quanto precisato dall'art. 94 PSD2) costituisce un consenso di natura contrattuale, che lega il prestatore di servizi di pagamento e il cliente, e sarebbe limitato al servizio di pagamento da svolgersi, diversamente dal consenso a cui fa riferimento il GDPR, che avrebbe, invece, un ambito applicativo più ampio[62]. A ciò consegue che il necessario consenso esplicito dell'utente di cui all'art. 29 del D.lgs. 11/2010, che legittimerebbe la condivisione dei soli dati necessari alla prestazione dei servizi di pagamento, si riferirebbe esclusivamente al trattamento dei dati direttamente correlato alla prestazione del servizio di pagamento richiesto dal cliente, mentre per gli ulteriori eventuali trattamenti dei dati bancari – compresa la cessione a titolo oneroso da parte del prestatore di servizi di radicamento del conto a terzi – troverebbero applicazione le regole generali di cui al GDPR.

A ben vedere, in applicazione dell'art. 6 comma 1 lett. a) GDPR, si potrebbe configurare in capo al prestatore dei servizi di radicamento del conto un diritto al trattamento dei dati personali altrui (del cliente), a condizione che il cliente abbia prestato un consenso espresso a favore del trattamento dei dati con tale finalità. Manca, però, una disposizione normativa che chiarisca se il cliente debba acconsentire espressamente alla cessione dei dati in favore di uno specifico acquirente dei dati o se sia sufficiente la prestazione del consenso per una generica finalità di cessione, anche a titolo oneroso, di tali informazioni a terzi.

Il Regolamento impone soltanto che il consenso prestato debba consistere in una prestazione di volontà specifica ed informata[63].

Non viene neppure chiarito se tali dati possano essere ceduti dal prestatore dei servizi di radicamento del conto anche in favore di soggetti

[62] M. Rabitti, *Il riparto di competenze tra Autorità amministrative indipendenti*, in M.C. Paglietti, M.I. Vangelisti (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento di interessi nella PSD2*, Roma, 2020, pp. 97 ss.

[63] L'art. 4, comma 1, n. 11) del GDPR si limita a chiarire che il consenso dell'interessato debba consistere in una manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato. In base alla diversa interpretazione del requisito della specificità consenso, potrebbe ritenersi sufficiente la prestazione del consenso dell'interessato (genericamente) alla cessione a titolo oneroso dei dati per fini commerciali o, altrimenti, dovrebbe ritenersi necessario l'espresso consenso alla cessione dei dati in favore di uno specifico soggetto cessionario. La *ratio* del requisito della specificità è quella di consentire al soggetto interessato di raffigurarsi, in modo inequivocabile, i possibili trattamenti a cui i propri dati potrebbero essere sottoposti.

differenti da banche e da prestatori di servizi di pagamento autorizzati: se tale soluzione non sembra ammissibile allorquando l'acquirente dei dati intenda utilizzarli per la prestazione di servizi di pagamento (rispetto ai quali sussiste un regime

di riserva di attività), non sembrerebbero esserci invece ostacoli ad ammettere la cessione di tali dati in favore di un soggetto che non sia autorizzato ex art. 114 *novies* TUB, qualora questi intenda farne un utilizzo non collegato alla prestazione di servizi di pagamento[64].

6. *(Segue) Le* digital commodities

La necessità di *compliance* con la *access to account rule*, come detto, ha determinato una decisa accelerazione nell'ammodernamento delle strutture tecnologica delle banche. L'innovazione tecnologica e lo sviluppo di operatori non bancari, che offrono servizi di aggregazione delle informazioni e altri servizi collegati a quelli di pagamento, favoriscono la maggiore concorrenzialità tra gli operatori (anche tra coloro che non siano inquadrabili esattamente nella medesima categoria imprenditoriale), dando vita – in alcuni casi – a veri e propri mercati nuovi, aventi ad oggetto beni ed utilità che dapprima non erano considerati tali[65] e che comunque erano privi di mercato.

Attesa la possibilità di cedere a titolo oneroso dati bancari – diversi ed ulteriori rispetto a quelli la cui condivisione è obbligatoria – dei propri clienti a favore di soggetti terzi, rispettando le condizioni di cui all'art. 6 GDPR, si deve valutare se le banche e i prestatori di servizi di radicamento di conti possano cedere, in massa e a fronte di corrispettivo, i dati relativi ad una pluralità di clienti, considerandoli alla stregua di vere e proprie *commodities*.[66]

[64] Sempre se il soggetto "acquirente" garantisca le condizioni minime di sicurezza nel trattamento dei dati personali.

[65] Sull'inquadramento teorico dell'informazione e la sua riconducibilità alla nozione di bene ampia è la letteratura. Tra gli altri, si segnalano P. Perlingieri, *L'informazione come bene giuridico*, *Rass. dir. civ.*, 1990, pp. 326 ss.; V. Zeno-Zencovich, *Sull'informazione come 'bene' (e sul metodo del dibattito giuridico)*, *Riv. crit. dir. priv.*, 1998, pp. 339 ss.

[66] Per *commodity* si intende una sostanza ottenuta industrialmente in grande quantità, in genere a basso costo, che costituisce la base per la produzione di molte altre sostanze. Sulla qualificabilità dei dati alla stregua di *commodities* si vedano, tra gli altri, H. Zech, *Data as a tradeable commodity*, in A. De Franceschi (a cura di), *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution*, Cambridge,

I dati dei clienti potrebbero rientrare nella nozione di *commodity* qualora siano considerati come beni infungibili e ceduti *in stock* da parte dei prestatori di servizi di radicamento del conto di pagamento. A ben vedere, però, occorre fare delle precisazioni, in ragione delle cautele previste dal legislatore con riferimento alla fase di raccolta dei dati.

Come chiarito nel paragrafo precedente, la circolazione di questi dati, in via di principio, non può prescindere dalla previa prestazione del consenso da parte del cliente a cui tali dati si riferiscono. Bisognerebbe domandarsi se il consenso prestato al TPP per la condivisione dei dati necessari per l'esecuzione di servizi di *payment initiation* e *account information* (obbligatoria e gratuita)[67] possa valere ad autorizzare – quando sia espressamente specificato – anche l'acquisto oneroso di ulteriori dati detenuti dal prestatore di servizi di radicamento del conto relativi al medesimo cliente (pur in mancanza di un esplicito consenso del cliente reso al prestatore dei servizi di radicamento del conto). In quest'ultimo caso, sarebbe comunque necessaria la prestazione di due consensi separati, poiché riferiti a diversi trattamenti dei dati, aventi peraltro differenti basi giuridiche.

A prescindere da tali interrogativi, affinché la cessione in massa possa essere considerata lecita, sarebbe necessaria la previa prestazione del consenso a tale trattamento dei dati personali da parte di ciascun cliente e ciò complica l'eventuale circolazione di tali informazioni. Tali difficoltà sono ulteriormente accentuate qualora si dovesse ritenere necessario che il soggetto interessato debba prestare espressamente il consenso alla cessione dei propri dati personali in favore di uno specifico cessionario, non essendo sufficiente il consenso ad una generica cessione degli stessi a titolo oneroso a terzi per finalità commerciali.

È chiaro, quindi, che al fine di poter disporre liberamente dei dati bancari dei propri clienti, le banche e i prestatori dei servizi di radicamento dei conti siano chiamati a realizzare una serie di attività onerose, volte a rispettare le previsioni del GDPR sul consenso al trattamento dei dati. Preme sottolineare come si tratti non di meri adempimenti formali, quanto piuttosto di attività volte a garantire una effettiva trasparenza e piena consapevolezza per il cliente dei trattamenti a cui i propri dati saranno (o potrebbero essere) sottoposti.

2016, pp. 51 ss.; A. De Franceschi, M. Lehmann, *Data as tradeable commodity and new measures for their protection*, in *The Italian Law Journal*, 2015, 1, pp. 51 ss.

[67] Con riferimento all'accesso delle terze parti ai conti, non è necessario che il cliente presti il proprio consenso (anche) al soggetto presso cui il conto è tenuto, ma è sufficiente che esprima il proprio consenso al AISP o PISP al momento della richiesta della prestazione del servizio.

Ebbene, l'effettivo espletamento di tali procedure potrebbe pregiudicare fortemente lo sviluppo di una libera *data driven economy*.

Parzialmente differente potrebbe, invece, essere l'ipotesi in cui il prestatore di servizi di radicamento del conto non ceda dati personali, bensì dati anonimizzati, cioè depurati da tutte le informazioni relative ai singoli clienti e non più riconducibili a questi ultimi. L'utilizzo che l'acquirente potrebbe fare dei dati anonimizzati e "spersonalizzati" è certamente diverso e più ridotto (in quanto riconducibile sostanzialmente all'analisi delle informazioni finalizzata a meglio calibrare i servizi da offrire sul mercato) rispetto a quello dei dati personali, ma la circolazione di queste informazioni non sarebbe soggetta alle stringenti regole di cui al GDPR sul trattamento dei dati personali[68].

Pur residuando perplessità, alla luce delle argomentazioni svolte, circa la possibilità di considerare, in via generale, il dato bancario come una vera e propria *commodity*, appare ad ogni modo evidente dall'analisi delle fonti normative di riferimento (PSD2 e GDPR) l'intento del legislatore europeo di spingere le banche ad adottare modelli di *business* che valorizzino le informazioni[69]. E dunque, il *favor* alla circolazione dei dati che emerge dalle fonti europee non trova piena realizzazione in ragione della necessaria osservanza della disciplina a tutela dell'interessato al trattamento, che mal si adatta all'esigenza di cessione in massa, ad una pluralità di cessionari, dei dati personali dei clienti delle banche e dei prestatori di servizi di radicamento dei conti.

7. *Conclusioni*

Il sistema del c.d. *open banking*, delineato dalla PSD2, realizza un *unbundling* della catena del valore[70] dei servizi di pagamento che, almeno

[68] Come evidenziato in Autorità garante della concorrenza e del mercato, *Indagine conoscitiva sui Big Data*, condotta congiuntamente con l'Autorità per le garanzie nelle comunicazioni e il Garante per la protezione dei dati personali, 2020, pp. 64 ss. Anche gli operatori che facciano uso di tecniche di anonimizzazione sono comunque tenute a valutare il rischio di re-identificazione e la "robustezza" delle metodologie impiegate per l'anonimizzazione dei dati. È stato, poi, chiarito che "né, sotto un diverso profilo, l'anonimizzazione dei dati può rappresentare un escamotage per effettuare trattamenti non compatibili con le finalità originarie della raccolta".

[69] Gammaldi, Iacomini, *Mutamenti nel mercato*, cit., p. 139.

[70] È stato messo in evidenza da M. Carney, *The Promise of FinTech – Something New Under the Sun?*, Deutsche Bundesbank G20 conference on "Digitising finance, financial

astrattamente, potrebbe determinare un aumento del volume complessivo delle transazioni e migliorare l'efficienza del sistema: al cliente potrebbero essere fornite migliori condizioni economiche (proprio perché questi avrebbe acceso, da una sola interfaccia, ai servizi offerti da una pluralità di operatori, con maggiori possibilità comparative) mentre le banche e le terze parti avrebbero un vantaggio in termini di maggiore redditività dei servizi offerti, potendosi concentrarsi sulla prestazione dei soli servizi relativi al proprio *core business*, lasciando che siano altri soggetti (specializzati) ad offrire altri servizi che si pongono lungo la catena del valore[71].

In tale contesto, assoluta centralità è assunta dai conti di pagamento, che sono considerati da taluni come vere e proprie *essential facilities*[72], in quanto strumento necessario ai fini dell'esercizio dei servizi di AISP e PISP (trattandosi di servizi *data-enabled*)[73]. Ben si capisce perché l'accesso ai conti non possa essere negato alle terze parti, che altrimenti sarebbero del tutto escluse dal mercato.

A ciò si aggiunge – in ipotesi – la possibilità per le banche di avere un'ulteriore fonte di guadagno nella cessione a titolo oneroso di determinati dati relativi ai conti di pagamento in favore di terze parti a ciò autorizzate.

---

inclusion and financial literacy", Wiesbaden, 25 gennaio 2017, <https://www.bis.org/review/r-38-.2b.pdf>, che la frammentazione della banca universale nelle sue varie *core functions* può avvenire grazie all'ingresso sul mercato di nuovi operatori e alla contestuale adozione, da parte degli *incumbents*, di nuove tecnologie che permettano di meglio perseguire i propri modelli di business, realizzando economie di scala.

[71] Cfr. Szego, *I nuovi prestatori autorizzati*, cit., 167. Effettuati gli adeguamenti tecnologici imposti dalla disciplina di origine europea, le banche dovranno decidere se svolgere le sole attività di esecuzione materiale delle operazioni negoziate da terze parti (con un esiguo margine di guadagno), o se divenire "driver dell'innovazione", offrendo servizi con un più elevato valore aggiunto (maggiormente remunerativi).

[72] Le innovazioni introdotte con la PSD2 determinano la creazione di una "platformification dei modelli di impresa". Cfr. S. Mezzacapo, *Competition policy issues in EU retail payment business: the new PSD2 regulatory principle of open online access to information from 'payment accounts' and associated 'payment transactions'*, in *European Competition Law Review*, 2018; P. Hines, *APIs in banking: unlocking business value with banking as a platform (BAAP)*, 2018.

[73] È stato, a tal riguardo, evidenziato da Burchi, Mezzacapo, Musile Tanzi, Troiano, *Financial Data Aggregation*, cit., p. 8; che i conti di pagamento non avrebbero soltanto la funzione di garantire la regolazione dei flussi di cassa, ma devono essere considerati "nella prospettiva di 'luogo' di 'registrazione' e di 'raccolta' di dati, connessi a scelte di consumo, risparmio o in senso più ampio 'finanziarie', che isolatamente o diversamente aggregate assumono anche la valenza di informazione 'ad alto valore aggiunto' con potenziali ulteriori destinazioni, trattamenti e utilizzi". La raccolta di tali dati permette lo sviluppo di nuovi mercati, sia *upstream* sia *downstream*.

Quest'ultimo profilo appare quello più innovativo nell'ambito della disciplina dell'*open banking*: le terze parti potrebbero avere interesse ad acquistare i dati personali dei titolari dei conti di pagamento al fine operare una profilazione dei clienti, personalizzando e migliorando così la propria offerta di servizi rispetto a quelli che avrebbero potuto fornire avendo accesso alle sole informazioni la cui condivisione è obbligatoria in base alla *access to account rule*; a ciò si aggiunga la possibilità che i terzi intendano acquistare dati bancari relativi a soggetti ulteriori, che non siano già loro clienti, così da proporre loro servizi in linea con le loro esigenze.

Come evidenziato, si tratta dell'aspetto dell'*open banking* di più difficile attuazione, proprio in ragione della complessa compatibilità di una siffatta operazione con la disciplina del GDPR.

Difatti, la commerciabilità del dato bancario relativo ai rapporti intrattenuti dal cliente con la banca – al di fuori del novero di dati di cui è obbligatoria la condivisione con i *Third Party Providers* in ossequio alla *access to account rule* – è sottoposto ad alcune formalità, in particolare quelle relative alla prestazione del consenso da parte del cliente per lo sfruttamento dei dati con finalità commerciali, che costituiscono un ostacolo alla diffusione del nuovo mercato dei dati bancari.

Assume poi rilevanza il profilo del *pricing* dell'accesso ai dati dei correntisti (la cui condivisione non è obbligatoria e gratuita): il rafforzamento delle sinergie tra prestatori di servizi di pagamento e terze parti potrà avvenire solamente qualora vengano definiti chiaramente – sulla base di parametri predefiniti – i costi di acquisto dei dati[74]. Fino a quel momento, la cessione dei dati relativi ai conti di pagamento sarà limitata dalle difficoltà e dalle tempistiche della negoziazione individuale (anche sul prezzo) dei dati di volta in volta compravenduti[75].

Alla luce delle considerazioni fin qui svolte, emerge che le limitazioni al trattamento dei dati personali poste dal GDPR pur non costituendo un ostacolo alla cedibilità dei dati bancari, rendono comunque più complessa e onerosa tale operazione e potrebbero, dunque, non consentire

[74] Si tratta di un profilo che necessita approfondimenti: è, infatti, necessario che vengano definite le modalità per la determinazione dei compensi delle banche così da rendere *"sostenibile il business model*" rendendolo rispondente alle *"esigenze di revenues*" come evidenziato da Rabitti, Sciarrone Alibrandi, *I servizi di pagamento*, cit., p. 3-1.

[75] Ulteriori limitazioni alla cedibilità dei dati riguardano, poi, le caratteristiche del cessionario dei dati: difatti, quest'ultimo dovrà necessariamente essere in grado di garantire il medesimo livello di tutela dei dati che la legge impone al titolare del trattamento che li abbia raccolti. Qualora questi non garantisca un siffatto standard, il trasferimento non potrà essere legittimamente effettuato."

la configurabilità del dato bancario come una vera e propria *digital commodity*, cedibile in massa e verso corrispettivo.

Il prestatore dei servizi di radicamento del conto (titolare del trattamento dei dati) non è, quindi, titolare di un diritto di disporre liberamente dei dati bancari dei propri clienti, in quanto l'ordinamento opera un bilanciamento tra due posizioni naturalmente contrapposte: da una parte, la protezione dei dati personali e, dall'altra, la costruzione di un "mercato digitale concorrenziale mediante la promozione della circolazione e della utilizzazione dei dati"[76].

Bibliografia

G. Alpa, *La proprietà dei dati personali*, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019.

Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, adottato il 9 aprile 2014, 844/14/EN WP 217, 23 ss.

Autorità garante della concorrenza e del mercato, *Indagine conoscitiva sui Big Data*, condotta congiuntamente con l'Autorità per le Garanzie nelle Comunicazioni e il Garante per la Protezione dei Dati Personali, 2020, pp. 64 ss.

D. Baldini, *Il difficile equilibrio tra consenso della persona interessata e legittimo interesse del titolare del trattamento: problemi e prospettive nei rapporti tra fonti interne e dell'Unione europea in tema di tutela dei dati personali*, in *Osservatorio sulle fonti*, 2017, 3.

O. Borgogno, *Regimi di condivisione dei dati ed interoperabilità: il ruolo e la disciplina delle A.P.I.*, in *Diritto dell'informazione e dell'informatica*, 2019, 3.

O. Borgogno, G. Colangelo, *Data, Innovation and Competition in Finance: The Case of the Access to Account Rule*, EU Law Working Paper n. /1, 2018.

F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018.

A. Burchi, S. Mezzacapo, P. Musile Tanzi, V. Troiano, *Financial Data Aggregation e Account Information Services. Questioni regolamentari e*

[76] G. Alpa, *La proprietà dei dati personali*, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, p. 20.

profili di business, Quaderni FinTech 0/2019 (https://www.consob.it/documents/46180/46181/FinTech_4.pdf/2adb8707-41bf-48a4-ad4e-ce8ecceoab13).

M. Carney, *The Promise of FinTech – Something New Under the Sun?*, Deutsche Bundesbank G20 conference on "Digitising finance, financial inclusion and financial literacy", Wiesbaden, .1 gennaio 2017, <https://www.bis.org/review/r170126b.pdf.>

A. De Franceschi, M. Lehmann, *Data as tradeable commodity and new measures for their protection*, in *The Italian Law Journal*, 2015, 1, pp. 51 ss.

D. De Paoli, *PSD2 e privacy*, in M.C. Paglietti, M.I. Vangelisti (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento di interessi nella PSD2*, Roma, 2020, 147.

G. Di Lorenzo, *Spunti di riflessione su taluni 'diritti dell'interessato'*, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, pp. 248 ss.

F. Di Porto, G. Ghidini, *'I Access Your Data, You Access Mine'. Requiring Data Reciprocity in Payment Services*, in *IIC – International Review of Intellectual Property and Competition Law*, 2020, 51, pp. 307-329.

L. Floridi, *Infosfera. Etica e filosofia nell'età dell'informazione*, Torino, 2009.

D.U. Galetta, *I principi di proporzionalità e ragionevolezza*, in M.A. Sandulli (a cura di), *Principi e regole dell'azione amministrativa*, Milano, 2015, pp. 69 ss.

F. Galgano, *Lex mercatoria*, Bologna, 2010.

D. Gammaldi, C. Iacomini, *Mutamenti nel mercato dopo la PSD2*, in F. Maimeri, M. Mancini (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, Quaderni di Ricerca Giuridica della Consulenza Legale della Banca d'Italia, n. 87, settembre 2019, pp. 123 ss.

I. Graef, M. Husovec, N. Purtova, *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law,* in *German Law Journal*, 2018, 19, 6, pp. 1359 ss.

P. Hines, *APIs in banking: unlocking business value with banking as a platform (BAAP)*, 2018 (https://www.fidor.com/documents/analyst-reports/celent-apis-in-bankingunlocking-business-v<alue-with-baap.PDF>).

F. Maimeri, M. Mancini (a cura di), *Le nuove frontiere dei servizi bancari e di pagamentofra PSD2, criptovalute e rivoluzione digitale*, in *Quaderni di Ricerca Giuridica della Consulenza Legale della Banca d'Italia*, n. 87, settembre 2019.

V. Meli, *Opportunità e sfide per la concorrenza nella disciplina dei servizi di pagamento*, in M.C. Paglietti, M.I. Vangelisti (a cura di), *Innovazione*

e regole nei pagamenti digitali. Il bilanciamento di interessi nella PSD2, Roma, 2020.
D. Messinetti, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, pp. 339 ss.
R. Messinetti, Circolazione dei dati personali e autonomia privata, in *Federalismi.it*, 21, 2019.
S. Mezzacapo, *Competition policy issues in EU retail payment business: the new PSD2 regulatory principle of open online access to information from 'payment accounts' and associated 'payment transactions'*, in *European Competition Law Review*, 2018.
M.C. Paglietti, M.I. Vangelisti (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento di interessi nella PSD2*, Roma, 2020.
G. Parker, M. Van Alstyne, S. Choudary, *Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You*, New York, 2016.
P. Perlingieri, *L'informazione come bene giuridico*, in *Rass. dir. civ.*, 1990, pp. 326 ss.
V. Profeta, *I third party provider: profili soggettivi e oggettivi*, in F. Maimeri, M. Mancini (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, in Quaderni di Ricerca Giuridica della Consulenza Legale della Banca d'Italia, n. 87, settembre 2019, pp. 47 ss.
M. Rabitti, A. Sciarrone Alibrandi, *I servizi di pagamento tra PSD2 e GDPR: open banking e conseguenze per la clientela*, in F. Capriglione (a cura di) *Liber Amicorum per Guido Alpa*, Padova, 2019.
M. Rabitti, *Il riparto di competenze tra Autorità amministrative indipendenti*, in M.C. Paglietti, M.I. Vangelisti (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento di interessi nella PSD2*, Roma, 2020, pp. 97 ss.
B. Russo, *L'evoluzione dei sistemi e dei servizi di pagamento nell'era digitale. Atti del Convegno nazionale in ricordo del Prof. Giuseppe Restuccia*, Padova, 2020.
A. Sandulli, *La proporzionalità dell'azione amministrativa*, Padova, 1998.
A. Sciarrone Alibrandi, *Impostazione sistematica della Direttiva PSD2*, in M.C. Paglietti, M.I. Vangelisti (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento di interessi nella PSD2*, Roma, 2020, pp. 13 ss.
J. Stylos, A. Faulring, Z. Yang, B.A Myers, *Improving API documentation using API usage information*, in *Proceedings of IEEE Symposium on Visual Languages and Human-Centric Computing*, Washington, 2009, pp. 119 ss.

B. Szego, *I nuovi prestatori autorizzati*, in M.C. Paglietti, M.I. Vangelisti (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento di interessi nella PSD2*, Roma, 2020.
S. Vezzoso, *Fintech, Access to Data, and the Role of Competition Policy*, in *Competition and innovation*, 2018, 7.
H. Zech, *Data as a tradeable commodity*, in A. De Franceschi (a cura di), *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution*, Cambridge, 2016, pp. 51 ss.
V. Zeno-Zencovich, *Prefazione*, in M.C. Paglietti, M.I. Vangelisti (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento di interessi nella PSD2*, Roma, 2020, pp. 10 ss.
V. Zeno-Zencovich, *Sull'informazione come 'bene' (e sul metodo del dibattito giuridico)*, in *Riv. crit. dir. priv.*, 1998, pp. 339 ss.
V. Zeno-Zencovich, *Cosa*, in *Digesto delle discipline privatistiche. Sezione civile*, IV, Torino, 1989.

Giorgio Resta

Pubblico, privato, collettivo nel sistema europeo di governo dei dati

Abstract: This paper investigates the collective dimension of data processing and focuses on the phenomena of data intermediation and data trust in the light of the EU Data Governance Act.

1. *L'articolazione del pacchetto digitale UE*

Il pacchetto digitale UE, nella sua attuale configurazione, poggia su tre pilastri fondamentali[1]. Il Digital Markets Act[2] è preordinato a limitare gli abusi di potere economico degli oligopoli digitali organizzati secondo il modello delle piattaforme. Il Digital Services Act[3] aggiorna la direttiva 2000/31/CE sul commercio elettronico, predisponendo un quadro regolatorio avanzato per il contrasto degli illeciti in rete e la responsabilità per contenuti informativi illeciti. Il Data Governance Act[4] (d'disciplina l'accesso ai dati del settore pubblico e introduce meccanismi di incentivazione alla condivisione dei dati in mano privata. Destinate ad integrarsi con tale impianto sono due ulteriori proposte normative di notevole momento, la Proposta di regolamento sull'intelligenza artificiale

* Questo articolo è stato originariamente pubblicato in *Rivista trimestrale di diritto pubblico*, 2022, pp. 971-995.

[1] P.G. Picht – H. Richter, *EU Digital Regulation 2022: Data Desiderata*, in *GRUR Int.,* 2022, 395.

[2] COM (2020) 842 final, testo adottato il 5 luglio 2022.

[3] COM (2020) 825 final, testo adottato il 5 luglio 2022.

[4] Regolamento (UE) 2022/868.

(AI Act) [5] e la Proposta di regolamento su accesso e uso dei dati (Data Act)[6].

Se si volesse cercare il filo rosso capace di illustrare la logica sottostante a interventi tanto articolati e complessi, questo andrebbe individuato nella sequenza dati-algoritmi-piattaforme: i dati come risorsa fondamentale dell'economia e della società digitale; gli algoritmi come strumenti capaci di estrarre valore da tali dati (anche per finalità analitiche, predittive e decisionali); le piattaforme come luoghi virtuali nei quali avvengono - intermediati in via algoritmica e con costante profusione di dati, riutilizzati per aumentare il potere delle piattaforme medesime – buona parte degli scambi e delle interazioni sociali contemporanee[7]. Su ciascuno di questi tre nodi si appuntano specifici segmenti di regolazione: Data Governance Act e Data Act si occupano di rimuovere le restrizioni non necessarie alla libera circolazione dei dati, per favorirne accesso e riuso[8]; l'AI Act (e prima ancora il GDPR) disciplina l'immissione in commercio e l'utilizzo degli algoritmi di intelligenza artificiale in una prospettiva di compatibilità con il quadro dei diritti fondamentali europei[9]; il Digital Markets Act e il Digital Services Act assoggettano le piattaforme al rispetto di determinati requisiti sia procedurali sia sostanziali al fine di salvaguardare il funzionamento delle regole di mercato e tutelare gli interessi dei terzi[10].

Per una valutazione più approfondita delle caratteristiche del modello di regolazione digitale UE, anche in chiave di confronto con gli itinerari emergenti su scala globale, sarebbe opportuno soffermarsi su ciascuno degli interventi citati, enucleandone le correlazioni e i sofisticati meccanismi di integrazione con il *corpus* normativo preesistente, dal GDPR alle regole in materia di concorrenza e proprietà intellettuale[11]. Questo è uno degli obiettivi che si propone il fascicolo nel quale si inserisce il presente contributo, che ha invece una finalità e un oggetto più limitati. In queste l'attenzione verrà ad appuntarsi soltanto sul primo dei tre nodi indicati, al fine di riflettere sul significato del Data Governance Act in ordine

[5] COM (2021) 206 final.

[6] COM (2022) 68 final.

[7] S. Grumbach, *L'empire des algorithmes. Une géopolitique du contrôle à l'ère de l'anthropocène,* Paris, 2022 ; J.E. Cohen, *Law for the Platform Economy,* in *U. Cal. Davis*, vol. 51, 133, 2017.

[8] H. Richter, *Europäisches Datenprivatrecht: Lehren aus der Kommissionsvorschlag* für eine „Verordnung über europäische Daten-*Governance",* in *ZEuP,* 2021, 634.

[9] G. Resta, *Cosa c'è di ' europeo' nella Proposta di Regolamento UE sull'intelligenza artificiale?,* in *Dir. inf.,* 2022, 323.

[10] M. Leistner, *The Commission's Digital Markets and Services Package – New Rules for Big Tech and Big Data,* in *GRUR Int.,* 2021, 515.

[11] Per un panorama più ampio v. B. Paal – L.K. Kumkar, *Die digitale Zukunft Europas. Europäische Strategien für den digitalen Binnenmarkt,* in *ZfDR,* 2021, 97.

all'evoluzione del sistema europeo di governo dei dati.

2. *Il diritto europeo dei dati e la sua evoluzione*

Iniziamo con un'osservazione banale, ma significativa. Nel diritto europeo mancava, sino all'entrata in vigore del Regolamento 2022/868 (Data Governance Act) una definizione normativa di 'dato'[12]. Sull'orizzonte legislativo si stagliava incontrastata la nozione di "dati personali", definita sin dalla Direttiva 1995/46/CE (art. 2, c. 1, lett. a) e poi dall'art. 4, n. 1, Regolamento (UE) 2016/679 come "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale". Tale definizione era di fatto destinata a condizionare qualsiasi discorso normativo sui dati, tanto che lo stesso Regolamento (UE) 2018/1807 "relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione Europea", non si scostava dal solco tracciato dalla direttiva 95/46 e dal GDPR. L'art. 3, n. 1, del Regolamento optava per una definizione di "dati" tutta costruita in negativo e in chiave oppositiva rispetto a quella di "dati personali", stabilendo che con l'espressione "dati" si intendono "i dati diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679".

Non si tratta di una circostanza dotata di un rilievo meramente lessicale, quanto di un indice piuttosto univoco del particolare equilibrio intorno a cui si è retto per lungo tempo il sistema europeo di governo dei dati. Questo ha visto in una posizione culturalmente e assiologicamente sovraordinata il compendio normativo concernente il trattamento dei dati personali, mentre un ruolo comparativamente minore è stato svolto da altri segmenti di disciplina, come quello relativo all'accesso ai dati, al riutilizzo delle informazioni del settore pubblico, o alla stessa proprietà intellettuale (con le specifiche propaggini delle discipline sulla tutela delle banche di dati e

[12] Mi era già occorso di segnalare tale circostanza in G. Resta, *Towards a unified regime of data-rights?* Rapport de synthèse, in T. Pertot (a cura di), *Rechte an Daten,* Tübingen, 2020, 231, 236.

del segreto industriale) [13]. Si potrebbe parlare, con qualche semplificazione, di un modello unipolare. Le ragioni sono agevolmente comprensibili e risiedono in larga parte nell'antecedenza storica della normativa in materia di trattamento dei dati personali, sviluppatasi sin dagli anni '70 prima in seno agli ordinamenti nazionali e poi gradualmente penetrata nel sistema del Consiglio d'Europa (Convenzione 108 del 1981) e dell'Unione Europea (a partire dalla direttiva 95/46/CE) [14]. I circa cinquant'anni di applicazione della normativa in oggetto, che peraltro ha implicato la creazione di apposite istituzioni deputate a assicurarne la supervisione e ha prodotto il sorgere di una comunità scientifica di specialisti della materia, hanno restituito ad essa caratteri di sistematicità, organicità e completezza che non è dato rinvenire nelle altre normative in tema di controllo delle informazioni. A ciò si aggiunga che sul piano dei principi, la disciplina della protezione dei dati personali si colloca senza dubbio ai vertici del sistema, in coerenza con un discorso pubblico che ha da sempre enfatizzato il legame di tali garanzie con il costituzionalismo post-bellico, sorto sulle macerie delle esperienze totalitarie novecentesche[15]. Ne è ora limpida testimonianza la scelta, compiuta dalla Carta dei diritti fondamentali UE, di prevedere in aggiunta al diritto al rispetto alla vita privata una specifica disposizione sul diritto alla protezione dei dati personali (art. 8). Tutto ciò si è tradotto in una posizione di primazia, sia sul piano della gerarchia delle fonti, sia su quello della compiutezza dell'elaborazione scientifica, della disciplina del trattamento dei dati personali rispetto agli altri campi del diritto preordinati a regolare la circolazione delle informazioni[16].

Non è forse azzardato prevedere che tale primazia sia destinata gradualmente ad incrinarsi sino a cedere il passo, per le ragioni che saranno di seguito illustrate, a un modello multipolare, nel quale le istanze di protezione dei dati coesisteranno con pari dignità con quelle di libero accesso e riuso dei dati medesimi[17]. A fianco a un *Datenschutzrecht* sembra

[13] In tema ampiamente T. Streinz, *The Evolution of European Data Law,* in P. Craig – G. de Búrca (a cura di), *The Evolution of EU Law*, III ed., Oxford 2021, 902 ss., 915; e ora P.C. Johannes, *Europäisches Datenrecht – ein Spickzettel,* in *ZD – Aktuell,* 2022, 1166.

[14] La ricostruzione più approfondita di questo percorso rimane quella di S. Rodotà, *Tecnologie e diritti,* II ed., Bologna, 2021.

[15] F. Bignami, *European versus American Liberty: A Comparative Analysis of Antiterrorism Data Mining*, 48 *B.C. L. Rev.* 609 (2007).

[16] T. Streinz, *op. cit*.

[17] Molto convincente al proposito appare l'impostazione metodologica di J. Drexl, *Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy,* in De Franceschi – R. Schulze, *Digital Revolution: New Challenges for Law*, München – Baden-Baden, 2019, 19, 21 ss.

emergere e acquistare giuridica consistenza un *Datenwirtschaftsrecht*[18].

La strategia europea dei dati[19] sembra preludere proprio a un siffatto percorso. Le scelte compiute con il Data Governance Act, destinate a essere ulteriormente integrate e sistematizzate con il Data Act (ancora allo stato di proposta della Commissione), rappresentano un primo passo in questa direzione. Non è quindi un caso che il DGA opti per una definizione autonoma di "dati" quali "qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva …" (art. 2, n. 1). Tale formula segna un distacco netto dalla pregressa impostazione da un lato perché delinea un *Oberbegriff* atto a ricomprendere al suo interno sia dati personali sia dati non personali; dall'altro perché mette in esponente la dimensione sintattica (per riprendere il linguaggio della scienza dei dati) dei dati[20]. In altri termini, mentre la nozione di dato personale si incentra sul carattere della riferibilità di una specifica informazione a un determinato individuo, esaltando così nella costruzione della fattispecie la dimensione semantica del dato quale latore di un'informazione, la formula accolta dal DGA – come già aveva fatto il nuovo Codice civile cinese[21] – prescinde da tale aspetto e accentua l'idea della "codifica" di stati del mondo tramite rappresentazione digitale[22]. Si coglie in ciò un sottile scivolamento della logica sottesa alla disciplina in oggetto: questa non è più volta a precostituire un meccanismo di salvaguardia di determinati beni incorporali in ragione del potenziale di conoscenza che essi possono sprigionare in relazione ad una persona. Prevale, invece, l'intento di prefissare un sistema di regole concernenti la circolazione e l'uso di dati in relazione alla loro strutturazione formale (e in particolare la leggibilità da un sistema automatico), indipendentemente dal tipo di significati che

[18] B. Steinrötter, *Das 'Datenwirtschaftsrecht' als neues Teilrechtsgebiet im Recht der Daten,* in *ZD,* 2021, 543; D. Staudenmayer, *Der Verordnungsvorschlag der Europäischen Kommission zum Datengesetz. Auf dem Weg zum Privatrecht der Datenwirtschaft,* in *EuZW,* 2022, 596.

[19] Si tratta della Comunicazione della Commissione del 19-2-2020, COM (2020) 66 final, *A European Strategy for Data.*

[20] Per questa distinzione v. H. Zech, *Besitz an Daten?*, in T. Pertot (a cura di), *Rechte an Daten,* cit., 21, 91; J. Drexl, *Designing Competitive Markets for Industrial Data. Between Propertisation and Access, JIPITEC,* 8 (2017), 257.

[21] Art. 127: „Where any laws provide for the protection of data and network virtual property, such laws shall apply"; in tema v. L. Yi, *Daten als eigentumsrechtlicher oder immaterialgüterrechtlicher Gegenstand in China*, in *GRUR Int.*, 2019, 238.

[22] Sul piano del linguaggio normativo, la prospettiva seguita dal DGA appare più convincente di quella adottata dal GDPR, anche per le ragioni evidenziate da M. Martini, *Datenhoheit. Annäherung an einen offenen Leitbegriff,* in *MMR-Beil.,* 2021, 3, 4.

questi siano atti a veicolare[23]. Sul piano teleologico, questo mutamento di impianto si riflette nel passaggio da una normativa essenzialmente limitativa ad una di stampo promozionale circa l'uso dei dati.

3. *Esclusione, accesso, condivisione: tre paradigmi per il governo dei dati*

La nuova strategia europea segna una forte discontinuità nel sistema di governo dei dati. L'approccio preesistente, posto a confronto con la nuova realtà tecnologica dei *big data* e dell'intelligenza artificiale, si è mostrato deficitario sotto molteplici punti di vista, ma soprattutto sotto i due profili dell'assenza di incentivi alla condivisione dei dati (personali e non personali) e dell'inefficacia dell'apparato di tutela rispetto alla realtà dell'*informational capitalism*.

Come osservato da Viktor Mayer Schönberger, le risultanze statistiche mostrano che circa l'85% dei dati raccolti in Europa non viene riutilizzato[24]. Tale circostanza è comune sia al settore dei dati personali, che, come ha mostrato l'esperienza pandemica, potrebbero essere reimpiegati con più efficacia per finalità di interesse pubblico, come la promozione della ricerca scientifica e il supporto alle politiche sanitarie; sia a quello dei dati non personali, quali ad esempio i dati industriali e i dati in possesso delle pubbliche amministrazioni. Ciò rappresenta di fatto un fattore frenante sul piano dell'innovazione, atteso che questa – e il riferimento non è limitato al settore industriale – è oggi in larga parte *data-driven.*

D'altro canto, anche nell'ambito normativo nel quale l'istanza preponderante è quella del controllo e non della condivisione, e segnatamente dei dati personali, il meccanismo di disciplina messo a punto dal legislatore europeo si è rivelato sotto alcuni aspetti inefficace al cospetto delle prassi organizzative e di mercato affermatesi nel contesto dell'economia digitale. In particolare, l'enfasi posta sin dalla Direttiva 95/46/CE sul meccanismo del consenso informato quale base normativa

[23] Sul punto B. Steinrötter, *Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts,* in *RDi,* 2021, 480, alla p. 481; F. Rosenkranz – M. Scheufen, *Die Lizenzierung von nicht-personenbezogenen Daten. Eine rechtliche und rechtsökonomische Analyse,* in *ZfDR,* 2022, 159, alla p. 168.

[24] T. Ramge - V. Mayer Schönberger, *Fuori i dati! Rompere i monopoli delle informazioni per rilanciare il progresso*, Milano, 2021, 39; v. inoltre per una dettagliata descrizione delle criticità dell'attuale sistema di governo dei dati, la già citata Comunicazione *A European Strategy for Data,* alla p. 6 e ss.

atta a legittimare il trattamento dei dati – al fianco di altri meccanismi legittimanti, compiutamente elencati negli artt. 6 e 9 Regolamento 2016/679 – ha innescato un processo di burocratizzazione del consenso sia nei rapporti con i soggetti privati sia in quelli con i soggetti pubblici[25]. Soprattutto, nel contesto dei rapporti online il consenso si è tradotto in quella famosa 'foglia di fico' a cui accennavano già molti anni addietro Guido Calabresi e Stefano Rodotà, atta a mascherare una realtà fortemente asimmetrica e in cui l'idea dell'autodeterminazione dell'interessato si è rivelata poco più che un'etichetta priva di riscontri operazionali[26].

Sono molteplici gli studi empirici che dimostrano come le c.d. *privacy policies* (informative nel linguaggio del legislatore) siano redatte in maniera talmente complessa e articolata che nella stragrande maggioranza dei casi (alcune indagini indicano il 75% dei casi) esse non vengono neanche lette[27]. E ciò peraltro è una scelta razionale, atteso che le chances di negoziazione dei termini del trattamento dei dati sono comunque molto basse, stante l'inclusione del consenso in moduli predeterminati unilateralmente (spesso volti a disciplinare anche altri aspetti del rapporto contrattuale, come il servizio di social network o la gestione di una casella di posta elettronica) e non suscettibili di modifica se non per aspetti marginali[28]. Inoltre, si è fatto notare che anche qualora il soggetto sia in grado di esprimere una consapevole determinazione di volontà nel rapporto con il primo titolare del trattamento (mercati primari), massima è l'opacità che regna sul resto della catena del valore e dunque sui successivi riutilizzi dei dati (mercati secondari) [29]. D'altronde è sotto gli occhi di tutti che i grandi oligopoli digitali hanno acquisito le loro sconfinato quote di mercato proprio grazie alle strategie di estrazione di valore dai dati delle persone, riguardati come risorse liberamente appropriabili[30]. Dunque, fra le critiche che più

[25] Sul punto v. C. Wendehorst – S. Schwamberger- J. Grinzinger, *Datentreuhand – wie hilfreich sind sachenrechtliche Konzepte?*, in T. Pertot (a cura di), *Rechte an Daten,* cit., 103 ss.

[26] S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, 47 ss., 133; Id., *Protezione dei dati e circolazione delle informazioni,* ora in *Tecnologie e diritti,* cit., 79 ss.

[27] T.J. Gerpott, *Datenschutzerklärungen – Materiell fundierte Einwilligungen nach der DS-GVO. Empirischer Forschungsstand und Verbesserungsfelder,* in *MMR,* 2020, 739.

[28] M. Kamp – M. Rost, *Kritik an der Einwilligung. Ein Zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen,* in *DuD,* 2013, 80 ss.

[29] C. Wendehorst – S. Schwamberger- J. Grinzinger, *Datentreuhand – wie hilfreich sind sachenrechtliche Konzepte?*, cit., 103 ss.; V. Zeno-Zencovich, *Do ‚Data Markets' Exist?,* in *MediaLaws,* 2019, 22 ss.

[30] In luogo di molti si veda l'approfondita indagine di J.E. Cohen, *Between Truth and Power: The Legal Construction of Informational Capitalism,* Oxford, 2019.

frequentemente vengono rivolte al modello europeo di protezione dei dati v'è quella per cui la normativa in oggetto mentre ha reso in certi casi più complicato il riutilizzo dei dati per finalità di pubblico interesse (si pensi unicamente al settore della ricerca biomedica, che soffre sia la mancanza di coordinamento a livello europeo del regime di riutilizzo dei dati, frammentato alla luce dell'art. 89 GDPR su scala nazionale[31], sia di insufficienti garanzie a livello locale[32]), al contempo non è riuscita ad opporre un argine robusto alle operazioni di parassitismo commerciale poste in essere a partire da risorse consustanziali alla sfera identitaria della persona.

4. *Dalla Strategia europea dei dati al* Data Governance Act

Si comprende quindi che la già citata Comunicazione della Commissione sulla Strategia europea dei dati[33] indichi la necessità di un cambio di rotta sotto ciascuno dei profili evidenziati, con l'obiettivo di non disperdere le opportunità create dalle tecniche dell'intelligenza artificiale e promuovere – a tutti i livelli - una maggiore circolazione e condivisione dei dati[34]. Il Data Governance Act raccoglie questa sfida operando su tre fronti principali: *a*) quello del riutilizzo dei dati in mano pubblica; *b*) quello dei servizi di intermediazione per lo scambio dei dati; *c*) quello della destinazione dei dati per finalità altruistiche.

4.1 *Il trasferimento dei dati tra il settore pubblico e il settore privato*

Le disposizioni che operano sul primo punto si muovono in una linea di continuità rispetto al *corpus* normativo preesistente, allargando la portata dei principi stabiliti dalle direttive su *open data* e riutilizzo delle informazioni del settore pubblico[35], sulla base della premessa che "i

[31] C. Wiese Svanberg, sub § 89, in C. Kuner – L. Bygrave *et al*. (a cura di), *The EU General Data Protection Regulation*, Oxford, 2020, 1240.
[32] G. Comandè, *Ricerca in sanità e data protection, un puzzle…risolvibile, in Riv. it. med. leg*., 2019, 187.
[33] COM (2020) 66 final.
[34] B. Steinrötter, *Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts,* cit. 483 ss.
[35] V. in particolare la direttiva 2019/1024. In tema R. Schildbach, *Zugang zu Daten der öffentlichen Hand und Datenaltruismus nach dem Entwurf des Daten-Governance-Gesetzes,*

dati generati o raccolti da enti pubblici o altre entità a carico dei bilanci pubblici debbano apportare benefici alla società" (cons. 6). Il DGA estende l'ambito di operatività di tali principi a determinate categorie di dati, e segnatamente quelli protetti per motivi di riservatezza commerciale, riservatezza statistica, tutela dei diritti di proprietà intellettuale o tutela dei dati personali (art. 3, c. 1). Il limite principale di tale modello è che non vengono prefissati specifici obblighi o garantiti diritti azionabili in ordine all'accesso ai dati pubblici per finalità di riutilizzazione, bensì sono semplicemente disciplinate agli artt. 4-8 le modalità con le quali può essere concesso il riutilizzo (divieto di accordi di esclusiva, requisiti inerenti il formato dei dati e la messa a disposizione, limite al trasferimento extra-UE, canoni concessori, sportelli unici)[36].

Si tratta di una linea giuspolitica coerente con l'impianto preesistente[37], ma probabilmente non tanto innovativa quanto quella perseguita dalla Proposta di Data Act, che piuttosto che insistere sul flusso dei dati *Government to Business*, sposta l'asse di incidenza normativo sull'opposto registro *Business to Government*[38]. Prendendo le mosse da una realtà operativa spesso connotata da una rilevante asimmetria tra i patrimoni informativi goduti da alcuni soggetti privati, granulari e continuamente aggiornati, e il patrimonio informativo pubblico, frequentemente disperso in silos informativi non comunicanti, la Proposta mette a sistema una serie di indici normativi già esistenti a livello nazionale (in particolare nel diritto francese) [39] ed europeo[40] e raccoglie alcune istanze emerse a livello di società civile soprattutto nell'ambito dei dibattiti sulle *smart cities*[41]. Essa codifica

in *ZD,* 2022, 148.

[36] Sul punto D. Tolks, *Die finale Fassung des Data Governance Act. Erste Schritte in Richtung einer europäischen Datenwirtschaft,* in *MMR,* 2022, 444, 445-446.

[37] A. Hartl – A. Ludin, *Recht der Datenzugänge. Was die Datenstrategie der EU sowie der Bundesregierung für die Gesetzgebung erwarten lassen,* in *MMR,* 2021, 534.

[38] D. Tolks, *Die finale Fassung des Data Governance Act,* cit., 449.

[39] Cfr. Art. 17 e ss. della *Loi pour une république numérique* del 7 ottobre 2016.

[40] Sul punto debbono confrontarsi soprattutto gli studi di H. Richter, *Zugang des Staates zu Daten der Privatwirtschaft,* in *ZRP,* 2020, 245; Id., *The Law and Policy of Government Access to Private Sector Data (B2G Data Sharing),* in Bundesministerium der Justiz und für Verbraucherschutz, Max-Planck-Institut für Innovation und Wettbewerb (a cura di), *Data Access, Consumer Interests and Public Welfare*, 2021, 529 <https://doi.org/10.5771/9783748924999-529> retrieved 29 April 2021; nonché A. Vigorito, *Government Access to Privately Held Data: Business-to-Government Data Sharing. Voluntary and Mandatory Models,* in 20 *Eur. J. Comp. L. & Governance* 1 (2022); e in prospettiva comparatistica F. Cate – J. Dempsey (a cura di), *Bulk Collection*, Oxford, 2017.

[41] V. ad es. E. Morozov – F. Bria, *Rethinking the Smart City. Democratizing Urban Technology,* Rosa Luxembourg Stiftung series, New York, 2018, 25 ss.

quindi il modello noto in letteratura come "reverse PSI" [42], delineando una fattispecie generale di trasferimento dei dati – sia non personali, sia personali previa pseudonimizzazione (Art. 17, c. 2, lett. d; art. 18, c. 5) – dal settore privato al settore pubblico[43].

Ciò segna una rilevante innovazione, almeno sul piano delle formule legislative, perché sinora si era sempre data la preferenza ad un modello di *data transfer* volontario[44]. Ove la Proposta dovesse essere approvata nei termini auspicati dalla Commissione, nelle ipotesi di "eccezionale necessità", puntualmente disciplinate all'art. 15, le pubbliche amministrazioni potranno far ricorso a un meccanismo autoritativo di accesso ai *datasets* privati, salva la corresponsione di un indennizzo – non dovuto soltanto nei casi di emergenza pubblica – comprensivo dei costi di duplicazione e trasferimento, nonché di un "margine ragionevole". La particolare rilevanza di questa norma si coglie dal fatto che tra le ipotesi di eccezionale necessità rientrano non soltanto i casi di prevenzione o gestione di un'emergenza pubblica, ma anche la circostanza per cui "l'assenza di dati disponibili osti all'attuazione di un compito di interesse pubblico stabilito per legge, i dati non siano reperibili sul mercato e l'adozione della procedura prevista dalla norma riduca significativamente gli oneri burocratici per i detentori dei dati". È evidente che in tal modo sono di fatto poste le premesse – sia pure in linea teorica – per una sorta di trasferimento coattivo dei dati per pubblico interesse, che potrebbe rappresentare il succedaneo dell'*eminent domain* nella società digitale. Non a caso è proprio su questa norma che si sono appuntate le prime notazioni critiche circa la Proposta[45].

4.2. *La dimensione collettiva: i servizi di intermediazione dei dati*

Sul secondo profilo si sofferma invece il capitolo III del DGA. Questo stabilisce i requisiti per i servizi di intermediazione dei dati, prescrivendo oneri procedurali di notifica (art. 11), condizioni sostanziali per la fornitura del servizio (art. 12), meccanismi pubblici di supervisione (artt. 13-14). È importante notare che, secondo la nuova definizione proposta nell'art. 2,

[42] Y. Poullet, *From* open data *to* reverse PSI – *A new European policy facing GDPR,* in *Eur. Public Mosaic,* n. 11, 2020.
[43] R. Podszun – C. Pfeifer, *Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission,* in *GRUR,* 2022, 952, 958.
[44] A. Vigorito, *Government Access to Privately Held Data: Business-to-Government Data Sharing. Voluntary and Mandatory Models,* cit., 14.
[45] R. Podszun – C. Pfeifer, *Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission,* cit., 958.

n. 11, si intende per servizio di intermediazione dei dati un "servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali". È significativo che siano espressamente esclusi dal perimetro della nozione i servizi che rappresentano il cuore del modello del capitalismo informazionale contemporaneo, come Google o Facebook, che raccolgono dati dagli utenti offrendo servizi formalmente gratuiti per poi conseguire profitti extra tramite la licenza a terzi dei dati aggregati, analizzati e organizzati in formato leggibile dalle macchine[46]. Ai sensi dell'art. 2, n. 11, lett. *a*), infatti, non rientrano tra i servizi di intermediazione i servizi che "ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati". Sottesa alla disciplina del DGA, come si osservava, è una finalità promozionale. Attraverso la predisposizione di un quadro giuridico certo e trasparente ci si propone di stimolare una maggiore condivisione dei dati, anche in continuità con la politica volta alla creazione dei nuovi specifici 'spazi europei dei dati' connotato ciascuno da proprie caratteristiche funzionali e regolamentari[47]. Uno dei presupposti fondamentali per conseguire tali obiettivi è aumentare la fiducia dei 'titolari' dei dati nella neutralità e nell'affidabilità del servizio di intermediazione (cfr. Cons. 5 e 32). Si comprende quindi che già sul piano definitorio siano stati esclusi i servizi che si basano sul modello dello sfruttamento industriale dei dati; e che il principio della neutralità sia stato formulato come primo tra i requisiti sostanziali da osservare per la fornitura del servizio[48]. L'art. 12, c. 1, lett. *a*), prescrive infatti che il fornitore del servizio di intermediazione "non utilizza i dati per i quali fornisce servizi di intermediazione dei dati per scopi diversi dalla messa a disposizione di tali dati agli utenti dei dati e fornisce servizi di intermediazione attraverso una persona giuridica distinta". Del pari, la lett. *m)* della medesima disposizione stabilisce uno specifico obbligo di natura fiduciaria per l'ipotesi in cui il servizio di intermediazione abbia ad oggetto

[46] In tema M. Hennemann – L. v. Ditfurth, *Datenintermediäre und Data Governance Act,* in *NJW,* 2022, 1905, 1908.
[47] Cfr. il Considerando 27 e v. D. Tolks, *Die finale Fassung des Data Governance Act,* cit., 446.
[48] Sul principio di neutralità M. Hennemann – L. v. Ditfurth, *Datenintermediäre und Data Governance Act,* in *NJW,* 2022, 1905, 1906.

dati personali, nell'intento di rafforzare ulteriormente la trasparenza e l'affidabilità del servizio: "il fornitore di servizi di intermediazione dei dati che offre servizi agli interessati agisce nell'interesse superiore di questi ultimi nel facilitare l'esercizio dei loro diritti, in particolare informandoli e, se opportuno, fornendo loro consulenza in maniera concisa, trasparente, intelligibile e facilmente accessibile sugli utilizzi previsti dei dati da parte degli utenti dei dati e sui termini e le condizioni standard cui sono subordinati tali utilizzi, prima che gli interessati diano il loro consenso".

Quest'ultimo rilievo induce a soffermarsi sulla tassonomia dei servizi di intermediazione proposta dal DGA e sul significato che essa assume nella prassi. L'art. 10, c. 1, contempla tre tipologie di servizi di intermediazione tra loro molto diversi.

i) La prima è quella incentrata sulla condivisione dei dati tra attori di mercato, per il tramite dell'interscambio o della costituzione di *data pools*. Nel linguaggio normativo si tratta di servizi di intermediazione tra "titolari dei dati" e "potenziali utenti" di essi, i quali "possono includere scambi di dati bilaterali o multilaterali o la creazione di piattaforme o banche dati che consentono lo scambio o l'utilizzo congiunto dei dati". Nella valutazione della Commissione, lo scambio B2B è ancora a un livello insoddisfacente e, se adeguatamente supportato, potrebbe ingenerare effetti positivi in termini di innovazione e offerta di servizi a valore aggiunto. Il problema fondamentale è che, in assenza di un diritto di esclusiva sullo sfruttamento dei dati industriali, sin qui opportunamente rigettato dal legislatore europeo[49], l'unico strumento di tutela è rappresentato dalla disponibilità materiale, e dunque dal potere di fatto vantato su tali risorse. Di conseguenza, sussiste una comprensibile ritrosia degli operatori economici a scambiare o mettere direttamente in condivisione i *datasets* più rilevanti, a meno che non siano assicurate idonee garanzie in punto di sicurezza della conservazione, limiti all'uso dei dati, assenza di conflitti di interesse, etc. Le condizioni stabilite all'art. 12 (in part. alle lett. *b*, *f-h*, *l*), sono mirate proprio a creare un terreno propizio alla messa in comune dei dati tramite una riduzione dei costi di transazione derivanti dalle asimmetrie informative[50]. Intermediari qualificati e dotati di adeguato capitale reputazionale, anche

[49] F. Rosenkranz – M. Scheufen, *Die Lizenzierung von nicht-personenbezogenen Daten. Eine rechtliche und rechtsökonomische Analyse,* cit., 168; B. Steinrötter, *Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts*, cit., 482; per ulteriori riferimenti al dibattito decennale sulla proprietà dei dati sia consentito rinviare a G. Resta, *Towards a unified regime of data-rights?* Rapport de synthèse, cit., 242.

[50] H. Richter, *Europäisches Datenprivatrecht: Lehren aus dem Kommissionsvorschlag für eine „Verordnung über europäische Daten-Governance",* cit., 643.

al di là delle esperienze esistenti dei *marketplaces* globali e delle piattaforme industriali di dati[51] – potrebbero favorire l'incontro tra domanda e offerta, contribuendo alla messa a punto di formati interoperabili e assicurando almeno indirettamente una forma di supervisione sull'uso dei dati[52].

ii) La seconda tipologia è quella consistente nei "servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi, permettendo in particolare l'esercizio dei diritti degli interessati di cui al regolamento (UE) 2016/679"[53]. Se nell'ipotesi precedente la preoccupazione principale è quella di stimolare la condivisione dei dati, in questo caso concorre l'esigenza di rafforzare l'esercizio consapevole del diritto di autodeterminazione informativa. Come si è osservato in precedenza, le caratteristiche più comuni dei mercati dei dati tendono a esaltare il divario di potere reale tra il singolo e le controparti professionali, rendendo la manifestazione del consenso poco più che un atto formale privo di reale valore decisionale[54]. Del pari, i diritti di cui agli art. 15 e ss. GDPR non sempre hanno un effettivo riscontro operazionale, o perché mancano gli incentivi necessari al superamento dei costi di inerzia coinvolti nell'esercizio del diritto o perché le stesse possibilità di supervisione circa le modalità di uso dei dati sono limitate. Di qui l'idea, da tempo avanzata, per cui il coinvolgimento di soggetti collettivi – come associazioni in tema di libertà civili, sindacati, etc. – in funzione di assistenza e supporti dei singoli interessati possa contribuire a rafforzare l'effettività dei rimedi in tema di trattamento dei dati[55]. Il DGA sembra muoversi su questa linea, prefigurando forme più o meno avanzate di supporto ai singoli individui sia nella fase antecedente alla manifestazione del consenso (art. 12, c. 1, lett. *m*; Cons. 30) sia in quella dell'esercizio dei diritti dell'interessato e dell'esperimento dei relativi rimedi (art. 2, c. 1, n.

[51] Per una descrizione dettagliata M. Hennemann – L. v. Ditfurth, *Datenintermediäre und Data Governance Act,* cit., 1906.

[52] M. Hennemann – L. v. Ditfurth, *Datenintermediäre und Data Governance Act,* cit., 1906, 1910.

[53] In tema F. Bravo, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contratto e impresa Europa*, 2021, 199 ss.

[54] Cfr. *supra*, par. 2.

[55] V. EDPS, *Opinion 9/2016 on Personal Information Management Systems. Towards more user empowerment in managing and processing personal data* (2016); C. Wendehorst – S. Schwamberger- J. Grinzinger*, Datentreuhand – wie hilfreich sind sachenrechtliche Konzepte?,* cit.

11; art. 10, c. 1, lett. *b*). Se lo schema è chiaro in termini generali, rimane da capire come si sposino tali regole con le forme organizzative riscontrabili nella prassi.

È opportuno distinguere a tal riguardo almeno due diverse ipotesi, connotate da caratteristiche funzionali profondamente differenti. La prima è riconducibile alla categoria nota come "personal information management services" [56], consistente nell'offerta al pubblico, per fini lucrativi, di servizi di gestione professionale dei dati (un esempio, recentemente portato all'attenzione del Garante per la protezione dei dati, è Weople) [57]. Questi possono comprendere strumenti tecnici per la personalizzazione delle dichiarazioni di consenso in ordine a specifici settori o trattamenti, attività preordinate alla negoziazione collettiva dei diritti al fine della monetizzazione dei dati personali, assistenza nell'esercizio dei diritti dell'interessato (si pensi tipicamente all'esercizio del diritto alla portabilità, di cui all'art. 20 GDPR). Nelle forme più avanzate, questa forma organizzativa potrebbe ricalcare il modello delle *collecting societies* del diritto d'autore[58]. La seconda è quella dell'amministrazione dei dati per finalità e in ambiti essenzialmente non lucrativi, come quelli della ricerca scientifica o delle politiche sanitarie. Molto diffusa a questo proposito, nei discorsi pubblici e nella letteratura scientifica, è la formula del *data trust* (o nella sua trasposizione tedesca *Datentreuhand*), che a sua volta può essere disarticolata in diverse tipologie operative, tutte connotate dal carattere fiduciario dei poteri ascritti al gestore e dalla segregazione del patrimonio informativo oggetto del *trust*[59].

iii) La terza tipologia è costituita dai servizi di cooperative dei dati[60]. Questi vengono definiti dall'art. 2, c. 1, n. 11 come servizi di

[56] B. Falkhofen, *Infrastrukturrecht des digitalen Raums. Data Governance Act, Data Act, und Gaia-X,* in *EuZW,* 2021, 787, alla p. 790.

[57] <https://weople.space>. Per approfondimenti su questo caso v. F. Bravo, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, cit., 216.

[58] L. Specht-Riemenschneider *et al., Die Datentreuhand. Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierung,* in *MMR-Beil.,* 2021, 25, alla p. 27.

[59] Su questa figura si v. in particolare L. Specht-Riemenschneider *et al., Die Datentreuhand. Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierung,* cit., 25 ss.; C. Wendehorst – S. Schwamberger- J. Grinzinger, *Datentreuhand – wie hilfreich sind sachenrechtliche Konzepte?*, in T. Pertot (a cura di), *Rechte an Daten,* cit., 103 ss.

[60] In generale v. H. Baars – A. Tank *et al., Cooperative Approaches to Data Sharing and Analysis for Industrial Internet of Things Ecosystems,* in *App. Sc.,* n. 11, 2021, 7547; M. Micheli *et al., Emerging models of data governance in the age of datafication,* in *Big Data*

intermediazione "offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali". Prevalente, in questa fattispecie, è la finalità mutualistica, in base all'assunto per cui creando una struttura collettiva e di coordinamento volta a socializzare il valore dei dati, i singoli membri di essa ne ricaverebbero un guadagno non soltanto in termini monetari, ma anche e soprattutto sul piano del controllo sulle modalità di trattamento e utilizzo secondario dei dati. Alcuni esempi emersi nella prassi, come quello delle cooperative dei dati create da conducenti di taxi (Driver's seat), da pazienti (salus.coop), o da pescatori (PescaData), mostrano come le cooperative di dati possano rappresentare, soprattutto a livello locale, un sistema interessante di gestione dei dati con carattere imprenditoriale ma alternativo rispetto agli schemi caratteristici del capitalismo estrattivo[61]. Non a caso è al modello delle cooperative di dati che si guarda con crescente interesse anche nei dibattiti sulle *smart cities*, dove questo viene proposto, assieme al *data trust,* come forma organizzativa contrapposta a quella dell'impresa lucrativa[62].

4.3. *La destinazione dei dati per finalità altruistiche*

L'art. 15 sottrae alla disciplina procedurale e sostanziale dei servizi di intermediazione le "organizzazioni per l'altruismo dei dati riconosciute",

& Society, July-December, 2020, 1, 7; S. Delacroix – N.D. Lawrence, *Bottom-up data trusts: Disturbing the 'one size fits all' approach to data governance*, in 9 *International Data Privacy Law* 236 (2019).

[61] Per un'attenta indagine sociologico-giuridica, v. E. Bietti – A. Etxeberria *et al., Data Cooperatives in Europe: A Legal and Empirical Investigation,* White Paper created as part of *The New School's Platform Cooperativism Consortium* and *Harvard University's Berkman Klein Center for Internet & Society* Research Sprint (Dec. 2021), accessibile all'indirizzo https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europe-group2.pdf.

[62] M. Petras, *Demokratischer Datenschutz. Kooperative Privatheit in der 'Smart City',* in *MMR,* 2021, 862, 864.

nonché le "altre entità senza scopo di lucro nella misura in cui le loro attività consistono nel cercare di raccogliere, per obiettivi di interesse generale, dati messi a disposizione da persone fisiche o giuridiche sulla base dell'altruismo dei dati". L'intento è quello di ritagliare un complesso di regole di favore per enti collettivi che, operando senza scopi di lucro, si propongano di stimolare la raccolta di dati personali e non personali e la loro destinazione a finalità di interesse generale[63]. Qui si innesta il terzo cardine su cui ruota l'impianto del DGA.

L'altruismo dei dati è definito dall'art. 2, c. 1, n. 16 come " la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale" [64]. Siamo fuori, evidentemente, dallo schema dell'intermediazione di mercato preordinata a stabilire modelli coordinati di sfruttamento (come nei *data pools*) o sistemi di monetizzazione dei dati collegati al loro reimpiego per scopi commerciali. Non siamo lontani, invece, dall'ipotesi del *data trust* – e le organizzazioni dell'altruismo dei dati ne rappresentano un chiaro esempio applicativo[65] – ferma restando la predeterminazione legislativa del tipo di finalità sottese all'intero schema negoziale, le quali debbono essere congruenti con l'interesse generale. L'esperienza della pandemia da Covid-19 ha avuto da questo punto di vista un rilievo centrale, perché ha fatto emergere l'importanza della condivisione dei dati, mostrando peraltro alcuni limiti del modello

[63] In tema P. v. Hagen – L. Völzmann, *Datenaltruismus aus datenschutzrechtlicher Perspektive. Wechselwirkung zwischen DGA und DS-GVO,* in *MMR,* 2022, 176.

[64] La disciplina dell'altruismo dei dati del DGA dà spessore normativo a un fenomeno ampiamente indagato in letteratura negli ultimi anni: v. tra i molti studi M. Taddeo, *Data Philantropy and Individual Rights,* 27 *Minds and Machines* 1 (2017); B. Prainsack, *Data Donation: How to Resist the iLeviathan,* in J. Krutzinna – L. Floridi, *The Ethics of Medical Data Donation,* Cham, 2019, 9.

[65] S. Kempny – H. Krüger – M. Spindler, *Rechtliche Gestaltung von Datentreuhändern. Ein interdisziplinärer Blick auf ‚Data Trusts',* in *NJW,* 2022*,* 1646, 1648.

del GDPR[66]. Si noti, ad esempio, che in Germania – dove il consenso dell'interessato è stato ritenuto base giuridica adeguata per il trattamento dei dati attraverso *tracing app*[67] – il Robert Koch-Institut ha promosso un'applicazione (*Corona-Datenspende*) volta a permettere la donazione da parte dei cittadini dei dati personali raccolti dai dispositivi intelligenti, quali ad. es. gli *smart watch*, per finalità epidemiologiche e di contrasto alla pandemia[68]. Del pari, diverse organizzazioni come Google o Facebook, hanno messo a disposizione dei governi i dati aggregati relativi alla mobilità della popolazione per individuare i *cluster* e seguire la diffusione del virus. Generalizzando tale modello, il DGA assegna uno specifico ruolo alle organizzazioni non lucrative impegnate sul fronte della raccolta e successiva destinazione dei dati per finalità di interesse generale, predisponendo un minuto apparato regolamentare che assicuri la trasparenza e l'indipendenza di tali organizzazioni, evitando la creazione di incentivi disallineati. Si prevede quindi innanzitutto un onere di iscrizione presso il registro pubblico delle organizzazioni di altruismo dei dati stabilito dall'art. 19 DGA. Questo è subordinato al possesso di una serie di requisiti specificati all'art. 18 (tra i quali lo scopo di lucro, la struttura funzionalmente separata per le attività in oggetto, il rispetto del codice contemplato all'art. 22). In secondo luogo, l'art. 20 impone il mantenimento di registri aggiornati, mentre l'art. 21 fissa una serie di obblighi e principi a tutela dei titolari dei dati, tra i quali l'obbligo di informazione (relativi agli obiettivi di interesse generale e alle successive vicende del dato), il rispetto della finalità nell'utilizzo dei dati, l'assistenza tecnica nella fase della prestazione o della revoca del consenso, la sicurezza nella conservazione dei dati. L'intento di fondo, coerentemente con quanto già osservato in merito ai servizi di intermediazione dei dati, è quello di corroborare la fiducia del pubblico nell'affidabilità di tali organizzazioni (cfr. Cons. 46), permettendo così alle altre forme di *nudging* che sostengono le motivazioni altruistiche (ad es. le campagne pubbliche di sensibilizzazione) di trovare un valido sistema di instradamento. Da notare inoltre la previsione, all'art. 25, di un modulo europeo di altruismo dei dati volto a permettere la raccolta del consenso in un formato uniforme presso tutti gli stati membri[69]; tema che solleva la

[66] K. Kuner, *Data Crossing Borders*, in *Verfassungsblog.de*, 15 aprile 2020.

[67] V. a questo riguardo D. Samardzic – T. Becker, *Die Grenzen des Datenschutzes – Der beschränkte Schutz durch Freiwilligkeit und Einwilligung bei Corona-Apps, EuZW*, 2020, 646.

[68] J. Kühling – R. Schildbach, *Corona-Apps. Daten- und Grundrechtsschutz in Krisenzeiten, NJW,* 2020, 1545, alla p. 1546; v. per informazioni attuali <https://corona-datenspende.de>.

[69] Sul punto, e per i problemi di rapporti con il GDPR, P. v. Hagen – L. Völzmann,

grande questione – ampiamente dibattuta soprattutto nel contesto della ricerca scientifica e malauguratamente lasciata irrisolta dal DGA (v. Cons. 50) – dei limiti di ammissibilità del c.d. *broad consent*[70].

Qui si arresta la portata dell'intervento europeo, sia perché non sono previste disposizioni puntuali né sui rapporti tra il 'donante' dei dati e le organizzazioni di altruismo, né su quelli intercorrenti tra tali organizzazioni e i terzi destinatari finali dei dati[71]; sia perché l'art. 16 è univoco nel rimettere agli stati membri l'adozione di politiche mirate di supporto all'altruismo dei dati, anche attraverso l'adozione di specifiche misure organizzative o tecniche.

5. *Luci e ombre del modello europeo*

Nel proporre una valutazione conclusiva dell'itinerario intrapreso con il DGA si deve necessariamente tratteggiare un quadro connotato da luci e da ombre.

Dal primo punto di vista, merita indubbio apprezzamento la linea di politica del diritto che sorregge il nucleo embrionale del nuovo diritto europeo dei dati, costituito dal DGA e destinato ad essere ulteriormente arricchito dal Data Act. Come si è illustrato in precedenza, questo non è più unicamente improntato a un'attitudine difensiva, ma persegue un intento di apertura dei silos informativi e messa a frutto del valore dei dati – personali e non personali – presenti in Europa attraverso la costituzione di spazi comuni di dati rimessi alla libera circolazione intracomunitaria. Tale progetto – che non va visto in autonomia, bensì in connessione con quello non meno importante concernente le infrastrutture digitali europee[72] – è cruciale sia sul piano della politica industriale, poiché nel medio periodo potrebbe contribuire alla riduzione della dipendenza strategica delle nostre imprese dalle grandi piattaforme di dati transnazionali[73], sia su quello delle politiche sociali, atteso che qualsiasi processo di innovazione volto a sfruttare le opportunità dischiuse dalle tecniche di intelligenza artificiale

Datenaltruismus aus datenschutzrechtlicher Perspektive. Wechselwirkung zwischen DGA und DS-GVO, cit., 177 ss.

[70] R. Schildbach, *Zugang zu Daten der öffentlichen Hand und Datenaltruismus nach dem Entwurf des Daten-Governance-Gesetzes,* cit., 151.

[71] *Ibid*.

[72] B. Falkhofen, *Infrastrukturrecht des digitalen Raums. Data Governance Act, Data Act, und Gaia-X,* cit., 791.

[73] In generale v. M. Denga, *Digitale Souveranität durch Datenprivatrecht?,* in *GRUR,* 2022, 1113.

richiede inevitabilmente la disponibilità di parchi di dati strutturati in formato leggibile dalle macchine e interoperabili. Ovviamente la specifica curvatura impressa al nuovo sistema europeo di governo dei dati non può implicare la radicale eliminazione delle garanzie – in particolare con riferimento al trattamento dei dati personali – costruite con fatica nel corso di un lungo processo di interazione tra diritto interno e diritto sovranazionale[74], ma richiede una delicata operazione di adattamento del quadro giuridico preesistente alla nuova realtà definita dalla transizione digitale.

È proprio in relazione a tale profilo che emergono alcune ombre dell'impianto regolatorio europeo. Un primo rilievo critico attiene all'eccessivo appesantimento burocratico e all'idea che la predisposizione di una cornice istituzionale adeguata possa di per sé condurre agli esiti auspicati dal legislatore. Complice il limite delle competenze unionali, non può certo ignorarsi che la semplice definizione di una nuova forma giuridica per i servizi di intermediazione o per le organizzazioni di altruismo dei dati non sia di per sé garanzia dell'attrattività sul piano costi/benefici di tali attività e dunque della loro effettiva intrapresa[75]. In assenza di adeguate politiche di incentivazione, in primo luogo di carattere fiscale, e in presenza di un fitto reticolato di obblighi procedurali e sostanziali che generano non irrilevanti oneri di *compliance*, non è remoto il rischio che l'impatto reale di tale disciplina risulti meno soddisfacente di quanto auspicato[76], anche perché per contendere il primato delle piattaforme transnazionali i nuovi soggetti dovrebbero fare scala e raggiungere livelli dimensionali e organizzativi elevati. Un secondo ordine di considerazioni, di tenore opposto, attiene alla difficoltà del sistema di coordinamento con il quadro normativo preesistente e alla portata ancora troppo limitata delle sue modifiche[77]. Uno dei problemi fondamentali da questo punto di vista è costituito dalla tensione intrinseca tra il GDPR e la normativa volta a incoraggiare la condivisione dei dati. La scelta del legislatore è stata quella di riaffermare, in caso di contrasto, la prevalenza del GDPR e di escludere che il DGA possa costituire una valida base giuridica per il trattamento, nonché influire

[74] In proposito v. A. Rossnagel, *Grundrechtsschutz in der Datenwirtschaft. Vorsorgeflichten in der Data-Governance,* in *ZRP,* 2021, 173.

[75] Sul punto ampiamente H. Richter, *Europäisches Datenprivatrecht: Lehren aus dem Kommissionsvorschlag für eine „Verordnung über europäische Daten-Governance",* cit., 646 ss.

[76] Così M. Hennemann – L. v. Ditfurth, *Datenintermediäre und Data Governance Act,* cit., 1910.

[77] B. Falkhofen, *Infrastrukturrecht des digitalen Raums. Data Governance Act, Data Act, und Gaia-X,* cit., 790.

su diritti e obblighi previsti dalla normativa sulla protezione dei dati (art. 1, c. 3). Il prevedibile effetto di un siffatto modello di interazione è quello di depotenziare gli strumenti messi in campo dal DGA per promuovere una maggiore circolazione dei dati.

Basterà considerare soltanto tre esempi, che appaiono particolarmente significativi.

Al primo si è già fatto cenno in precedenza, trattando delle organizzazioni di altruismo dei dati[78]. L'idea della 'donazione' dei dati per determinate finalità di interesse generale è di per sé interessante e atta a colmare il divario tra la disciplina del corpo (incentrata sul modello del dono solidaristico) e quella dei dati[79]. Tuttavia, in assenza di disposizioni di natura sostanziale che circoscrivano il requisito della specificità del consenso e ammettano la possibilità di destinare dati personali per scopi altruistici a ambiti o linee di ricerca o altre politiche sociali, con effetto di armonizzazione sovranazionale, l'altruismo dei dati rischia di tradursi in una mera formula di facciata, un dispositivo di *marketing* normativo privo di significativo impatto operazionale[80].

Il secondo esempio concerne il rapporto tra intermediari dei dati e esercizio dei diritti dell'interessato (lo stesso tema emerge in relazione all'autorizzazione al trattamento dei dati, ma verrà trattato di seguito). Perché i fiduciari possano adempiere efficacemente i compiti loro assegnati parrebbe importante riconoscere in capo a costoro la facoltà di sostituirsi all'interessato nell'esercizio dei diritti ex art. 15 e ss. GDPR[81]. Tuttavia, è dubbio che tale soluzione sia praticabile alla luce del diritto vigente. Da un lato il DGA usa espressioni ambigue, che riflettono una malcelata incertezza circa la natura dei poteri vantati dai fiduciari. L'art. 2, c. 1, n. 11, nel definire i servizi di intermediazione dei dati, fa riferimento a una funzione strumentale all'instaurazione di rapporti commerciali tra gli interessati e gli utenti dei dati "anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali". Il Considerando n. 30, dopo aver premesso che il ricorso a servizi di intermediazione potrebbe permettere di "rafforzare la capacità di agire degli interessati e, in particolare, il controllo dei singoli individui in merito ai dati che li riguardano", prospetta un mero ruolo di assistenza. Si afferma infatti che gli intermediari "assisterebbero

[78] Cfr. *supra,* par. 4.3.

[79] In proposito v. G. Resta, voce *Contratto e diritti fondamentali,* in *Enc. Dir. – I tematici,* I, *Contratto,* Milano, 2021, 291 ss., 302, 306.

[80] Così anche R. Schildbach, *Zugang zu Daten der öffentlichen Hand und Datenaltruismus nach dem Entwurf des Daten-Governance-Gesetzes,* cit., 152 ss.

[81] C. Beise, *Datensouvernaität und Datentreuhand,* in *RDi,* 2021, 597.

i singoli individui nell'esercizio dei loro diritti a norma del regolamento (UE) 2016/679, in particolare gestendone la concessione e la revoca del 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 alla limitazione del trattamento e il diritto alla portabilità dei dati". Benché la terminologia impiegata sia tutt'altro che inappuntabile, sembrerebbe che le formule utilizzate evochino l'idea di una amministrazione meramente tecnica di determinazioni di volontà riferibili all'interessato (il modello sembra essere quello dei "personal information management services"), così confermando l'idea dell'assenza di autonomo potere decisionale in capo al fiduciario. Dall'altro lato, un'interpretazione diffusa dell'art. 80 GDPR, enfatizzando la lettera del primo comma, limita la possibilità di conferire mandato a enti e organizzazioni collettive soltanto in ordine alla proposizione del reclamo e all'esperimento dei rimedi giurisdizionali di cui agli artt. 77 e ss. GDPR, escludendo invece l'ipotesi dell'esercizio dei diritti di cui agli artt. 15 e ss. [82] Premesso che a chi scrive una siffatta interpretazione non appare né obbligata né persuasiva – l'apparente lacuna può essere ragionevolmente colmata attraverso un'applicazione analogica dell'art. 80, c. 1[83] – è innegabile che una più coraggiosa formulazione del DGA avrebbe contributo a rimuovere tale incertezza e legittimare una soluzione più funzionale agli scopi perseguiti (peraltro perfettamente in linea con le stesse indicazioni della legge 675/1996 che all'art. 13 prevedeva espressamente il diritto di conferire mandato a enti collettivi per l'esercizio dei diritti dell'interessato).

L'ultimo esempio concerne le cooperative di dati. Qui si deve innanzitutto osservare che, sul punto dell'esercizio dei diritti dell'interessato *ex* art. 15 e ss. GDPR, il testo finale del DGA segna un progresso significativo rispetto all'originaria Proposta della Commissione. Difatti, il Cons. 24 della Proposta, specificamente concernente le cooperative, affermava: "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" [84]. Il riferimento al "conferimento" e alla "delega" è scomparso dal testo finale

[82] Si registrano però alcune aperture sul punto da parte dell'EDPB, *Guidelines 01/2022 on data subject rights – Right of access,* 18 january 2022, 27.

[83] L. Specht-Riemenschneider *et al., Die Datentreuhand. Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierung,* cit., 43.

[84] In adesione a questa soluzione restrittiva v. EDPB-GEPD, *Parere congiunto sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati*, 2021, 35.

del Regolamento. Nel corrispondente Cons. 31 si legge ora, invece, che "i diritti a norma del Regolamento (UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunziarvi". Sebbene gli esercizi di esegesi delle norme di matrice europea sulla base delle categorie del diritto interno debbano sempre essere condotti con grande prudenza, sembrerebbe ragionevole ritenere che mentre il divieto della rinunzia, quale tipico atto abdicativo, implichi l'impossibilità del conferimento in società (atto con efficacia reale), esso non preclude invece la stipula di un contratto di mandato (con rappresentanza), in quanto atto con mera efficacia obbligatoria. Sembrerebbe quindi aprirsi un più ampio spazio operativo quanto meno per la tutela esterna dei diritti degli interessati da parte di una cooperativa di dati che operi come rappresentante dei suoi membri[85]. Ciò detto, si apre un secondo problema, che attiene non tanto al profilo negativo della tutela, quanto a quello positivo dello sfruttamento mediante attività negoziale con terzi. La logica stessa di una compagine con scopo mutualistico suggerirebbe l'opportunità di riconoscere un conferimento dei dati con correlativi poteri dispositivi in capo alla società. Tuttavia le formule legislative sembrano escludere una siffatta possibilità, sia perché tra gli obblighi imposti ai servizi di intermediazione v'è quello della neutralità (art. 12, c. 1, lett. *a*), così da escludere qualsiasi attività di *data analytics* prodromica ad un'efficace attività negoziale con terzi (questa ad esempio è la logica organizzativa di Drivers' seat e di altre cooperative nel settore della mobilità) [86]; sia perché il DGA in diversi punti sembra espressamente limitare il ruolo delle cooperative – e a maggior ragione degli altri intermediari dei dati – a un'attività di consulenza precedente alla manifestazione del consenso, o al massimo a quella di trasmissione a terzi della manifestazione di volontà dell'interessato[87]. Il consenso, in altri termini, figura nell'impianto del DGA come atto personale non delegabile a terzi. Nel Considerando 31 è contemplato tra gli obiettivi della cooperativa quello di "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, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori

[85] Su questo problema v. L. Specht-Riemenschneider *et al., Die Datentreuhand. Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierung,* cit., 41 ss.

[86] Sul punto E. Bietti – A. Etxeberria *et al., Data Cooperatives in Europe: A Legal and Empirical Investigation,* cit., 17-18.

[87] Così, criticamente, M. Denga, *Digitale Souveranität durch Datenprivatrecht?,* cit., 1118.

ai singoli membri del gruppo"; nell'art. 12, c. 1, lett. *m,* nel delineare il contenuto fiduciario dei doveri gravanti sugli intermediari di dati personali (tra i quali rientrano le cooperative), contempla specifici compiti di consulenza, in modo tale da fornire agli interessati adeguate informazioni sulle proposte negoziali dei terzi "prima che gli interessati diano il loro consenso". D'altronde già sul piano della teoria generale del consenso al trattamento dei dati, è prevalente – ma non unanime – l'opinione che esclude la possibilità di rappresentanza, riconoscendo a tale atto natura personalissima[88]. Non c'è quindi da stupirsi per la timidezza mostrata dal legislatore del DGA, anche se bisognerebbe riconoscere che lo strumento della cooperativa dei dati, per conseguire efficacemente i propri scopi sociali e per contendere il primato del modello imprenditoriale lucrativo, necessita un più ampio margine di azione e un quadro giuridico abilitativo[89]. È per questa ragione che lo stesso totem della natura personale del consenso, che pure costituisce un baluardo dell'autodeterminazione nell'ambito dei rapporti di mercato, trasposto alla sfera dei rapporti fiduciari e ai sistemi di imprenditoria sociale, meriterebbe forse di essere superato. D'altronde l'intera esperienza della negoziazione dei diritti della personalità ha fatto emergere, nelle pieghe delle declamazioni dottrinarie, spazi inaspettati di esercizio dell'autonomia privata (si pensi alla concessione di licenze con effetti reali)[90], che richiedono di essere opportunamente valorizzati, sì da riconoscere la possibilità di rappresentanza nell'espressione del consenso al trattamento dei dati, con il solo limite della soggezione della procura dei requisiti fissati dall'art. 7 GDPR, e in particolare a quello della specificità[91]. D'altronde l'art. 8 GDPR prevede espressamente che gli esercenti la potestà genitoriale possano validamente esprimere un consenso per il minore d'età, e il mero silenzio in ordine all'ipotesi della rappresentanza volontaria non può essere di per sé inteso come un divieto[92].

In conclusione, l'itinerario intrapreso a livello europeo merita nel complesso apprezzamento, ma si deve auspicare un ulteriore sforzo nel

[88] S. Ernst, *Die Einwilligung nach der Datenschutzgrundverordnung,* in *ZD,* 2017, 110, alla p. 111.
[89] E. Bietti – A. Etxeberria *et al., Data Cooperatives in Europe: A Legal and Empirical Investigation,* cit., 18.
[90] Sia consentito il rinvio a G. Resta, *Autonomia privata e diritti della personalità,* Napoli, 2005, 320 ss.; V. Zeno-Zencovich, *Profili negoziali degli attributi della personalità*, in *Dir. inf.*, 1993, 545.
[91] L. Specht-Riemenschneider *et al., Die Datentreuhand. Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierung,* cit., 41-42.
[92] *Ibid.*

valorizzare la dimensione relazionale e collettiva del trattamento dei dati[93], anche aprendo con più decisione all'autonomia contrattuale, oltre le strettoie imposte da una lettura eccessivamente individualistica del sistema delineato dal GDPR. Se non si compie un passo più deciso in questa direzione, non si vede come si possa sciogliere la contraddizione di fondo derivante dal fatto che il DGA e il Data Act intendono creare un mercato dei dati, mentre la normativa di *Datenschutz* è mirata a sottrarre i dati al mercato.

[93] S. Viljoen, *A Relational Theory of Data Governance,* in *Yale L.J.*, vol. 131, 573, 2021.

SECTION V

Data Protection and Privacy

Giorgio Resta, Vincenzo Zeno-Zencovich

Rise and Fall of Tracing Apps

Abstract: This paper provides a retrospective analysis of the spread of tracing apps in Western countries as a tool aimed at countering the Covid-19 pandemic, and explains, mainly from a comparative law perspective, why this experiment turned out to be a failure.

1. *Introduction*

When in March 2020, the COVID-19 pandemic erupted in Europe with thousands of casualties every day and extreme difficulty in preventing it from spreading even more violently, great hope was put in so-called 'tracing (or tracking) apps', already experimented in some Asian countries (China, South Korea, Singapore).

The idea behind the app (and in particular the Bluetooth Low Energy app) was simple: one downloaded the app in one's smartphone. If one resulted positive to the COVID-19 virus, one alerted the system, and all those who had downloaded the app and had been for a certain time (approx. 15 min) and at a short distance (approx. 1–2 m) from the infected person were warned of a possible occasion of contagion and invited to verify their positivity/negativity and to self-quarantine.

Rapidly the various European countries selected a model of the app. The EU issued lengthy normative texts meant to provide general guidance and promote uniformity and compliance with community laws.

When, towards the end of April 2020, the various applications started to rollout, the response was extremely slow and limited. The number of those joining the programme increased, but certainly not skyrocketed even following the upsurge of the pandemic in its second and deadly wave in Autumn 2020. One can, very frankly, say that anti-COVID tracing apps have been an almost complete failure.

In this short paper, we would like to succinctly point out some of the possible causes and what lessons may be learnt for the future.

* This article was first published in *Privacy and data protection in software services,* Cham: Springer Verlag, 2021, pp. 153-162.

2. *The Complexity of Legal Transplants*

Since the very beginning of the European debate on tracing applications, the East-Asian experience has been taken as a reference model in a quite simplistic manner, without carefully reflecting on the peculiar institutional framework surrounding the use of tracing apps in those systems and conditioning the efficacy of a legal transplant.

First of all, it deserves to be noted that tracing apps were not the only and not even the most important of the digital solutions adopted in the East with the aim of countering the pandemic. Migration maps created by integrating different sources of data, last generation screening technologies (such as body temperature scans), AI models applied to health data for the purposes of diagnosis and risk prediction, electronic monitoring of home-quarantined individuals, health QR codes, virtual care platforms, robots for personal care in hospitals, all of the above are just some examples of the panoply of digital technologies effectively deployed since the very first stage of the pandemic. Secondly, to correctly appreciate the effectiveness of East-Asian strategies, one should keep in mind that COVID-19 was just the last episode of a long wave of health crises triggered by contagious diseases experienced in recent times in that region. China, Hong Kong, South Korea were already faced with the need to restructure the whole framework of disease control first in 2002 following the outbreak of the SARS epidemic, and later in 2013 of the MERS (which hit South Korea). This led to a revision and modernization of the respective legislations on disease control, which proved extremely helpful for the fight against COVID-19. In China, the general *Law on Prevention and Treatment of Infectious Diseases* (1989) was deeply revised in 2004 and later amended in 2013. Together with the 2003 *Law on Emergency Response* and the 2003 regulation on *Contingent Public Health Emergencies*, this statute provided themain legal framework for rapidly adopting a set of wide-ranging measures, such as the blockading of entire areas, cities or regions of the country, the building of dedicated hospitals and the development of online healthcare platforms (measures rapidly put in place in the citiesmost hardly hit by the pandemic, such as Wuhan). In South Korea, the *Act on Infectious Diseases Prevention and Control* was amended in 2015, with the aim of improving the responses to the possible outbreak of new contagious diseases. The new Articles 34 *bis* and 76 *bis* of the Act make massive recourse to various sources of data for tracking purposes possible. In particular, they grant public authorities the power to

access a wide gamut of personal data—geolocation data, communications metadata, history of purchases and financial data, health data, video surveillance footage—with the aim of tracking the patterns of the disease and informing the public through detailed migration maps.

As a result of this background, South Korea and China were extremely fast and efficient in adopting a wide range of measures—physical and digital—as soon as the COVID-19 epidemic erupted. Lastly, it is worth underlining that tracing applications are embedded in a cultural and legal framework whose features mark a stark contrast, from the several points of view, with the European tradition. Among such features are the following: (a) quasi-compulsory use of digital tools, as evidenced by the Chinese resorting to the QR Code as a requirement to access public places; (b) loose application of data protection principles vis-à-vis public authorities, as evidenced

by the Chinese and Singaporean experience; (c) adoption of centralized models of tracing applications and access by health authorities to proximity data (Singapore); (d) strict surveillance and harsh enforcement of quarantine obligations. Since most of these features appear to be in contrast not only with the GDPR, as will be later detailed, but also with the general framework of European fundamental rights (see in particular art. 8 ECHR and art. 8 European Charter Fundamental Rights), the transplant of the techno-legal model 'tracing app' was necessarily a selective and highly ineffective one.

3. *Technical Inadequacies*

It would appear that one of the essential features of all tracing apps was that the smartphone in relation to proximity should have activated the Bluetooth application enabling a reciprocal connection. However, Bluetooth is an energy-consuming technology which renders it not very attractive especially for thosewho are in possession of old devices and are in open spaces. Furthermore, Bluetooth compared to the GPS has the advantage of being a less privacy-intrusive technology, as it does not disclose the location of its user, but only the distance and duration of the exposure.

However, tracing applications based on Bluetooth—a technology developed to make communications between two devices possible—have strong limitations in terms of precision of measurements (more so if the

sensors built in the smartphones are not of the last generation) and are prone to false positives. For instance, the presence of a wall or a Plexiglas shield between the two devices would not be recorded by the system. Lastly, BLE applications can detect proximity as long as the smartphone is switched on and carried by its user; if these conditions are not given, then the tracing app would be unable to detect proximity, both active and passive. It is no wonder, therefore, that alternative solutions, such as cheap wearable devices independent from any smartphone, have been proposed and carefully considered by the decision-makers.

4. *Digital Divide*

The tracing apps were developed for the current generation of smartphones. This clearly cut out all the holders of less recent devices, and in particular traditional mobile phones, not connected to the internet, and very common among elderly persons, the most exposed to infection and its dire consequences. Obviously, it also cut out all the persons not owning a cell phone, like children and the very poor.

5. *Organizational Failures*

To be effective, a tracing app requires around it—as anticipated above—an efficient health prevention system. Not only is it necessary that the person who has resulted positive in the COVID-19 test alerts the system, but it is necessary that this rapidly detects those who have been in his/her proximity. If the alert arrives many days later, the prevention effect is substantially watered down, with a chain reaction: those who have been in contact with a person who results positive will know if they have been infected only several days later, and in the meantime, may have infected many others.

The Italian experience is illustrative. At least during the first and the second wave of the pandemic, the Italian screening system was under pressure, and due to serious organizational deficiencies, people had to wait long hours to get tested and several days to get the results. This meant that an alert could have been sent days after the appearance of symptoms.

Furthermore, doctors and other personnel in charge of the unlocking of the app and the sending of an alert had not been properly instructed and, in several cases, proved unable to initiate the notification proceeding.

6. *The GDPR Totem*

However, the principal reason for the failure of tracing apps in the EU appears to be the concerns—real or supposed—related to respect of privacy, and more specifically compliance with the GDPR. Clearly tracing apps collect, directly or indirectly, personal data on the location, movements and activity of those who have downloaded them. If and when an individual test is positive and alerts the system, the data are of sensitive nature and therefore, undergo special requirements in its processing. The consequences that the GDPR has had on the roll-out of the tracing apps appear to be manyfold:

a) The GDPR is a mastodontic piece of legislation that covers many layers of public and private actions. The COVID-19 pandemic has shown that it is overly constraining and to a certain extent unworkable in an emergency. With the risk of enormous sanctions (economic, administrative and even criminal), an ordinarily cautious public or private decision-maker is naturally nudged towards a work-by-the-rule approach. The very aggressive stance that EU authorities and national data protection agencies have had during these last years has had a highly deterrent—if not chilling—effect. Just to give one example, the processing of data for scientific research, and in particular, the cross-border transfer of samples and data for studies related to COVID-19, has been obstructed and made more burdensome given the not-so-clear legal basis offered by Article 49 GDPR.

b) The clearest result of such a privacy-above-all approach is the decision of the producers of the main anti-COVID-19 tracing app, Google and Apple, to favour a decentralized model: the data concerning the holder of the smartphone and his or her contacts remain strictly under the holder's control. Only if he or she decides to inform on a COVID-19 positivity, does the system enter in action sending the alerts to the eventual contacts. Furthermore, the collection of GPS data from telecommunication providers has been limited to

exceptional cases, and this has impeded the creation and disclosure of migration maps such as those employed in South Korea. This solution is highly inefficient because it relies on individual choices for the success of a public health strategy. However, it is understandable that the companies—constantly under fire as members of the GAFAM 'villain group'—were not willing to develop different apps that hypothetically could have brought them into further regulatory troubles. Also, they had a specific interest in entering the promising commercial field of eHealth and at the same time marketing their position as inflexible guardians of privacy, who would never agree to transfer sensitive data to the governments.

c) Data protection is presented as a distinctive feature of the EU constitutional (Article 7 of the CFREU) and institutional (EDPS, EDPB) framework. It is one of the bastions of the 'European fortress' used to protect the EU from data appropriation and exploitation by big-tech giants from the East (China) and the West (the already mentioned GAFAM). With all the rhetoric behind personal data protection, enhanced by scores of hardline decisions of the CJEU, a flexible and realistic approach was untenable.

d) The rhetoric of the GDPRhas invaded and infected public and private discourse: millions of citizens who every second of their daily life provide thousands of personal data to all the private online business (not only the big-tech giants but also any provider of apps or online services), enabling them to profile them in every aspect, raised the alarm over a revised and incumbent version of the Orwellian Big Brother. The individual right to privacy became the antagonist of public health concerns which had to surrender. The cleavage between individualist (and selfish) EU societies and community-oriented (and rigidly governed) Eastern ones has become ever wider.

e) The result is that an app that in order to be effective needed to be downloaded and kept constantly in function by at least two-thirds of the adult population, in its peak reached not more than 30% of the citizens of a well-organized and disciplined country such as Germany and an average 15% in the others. It should have been compulsory and centralized (along the lines of the East-Asian experience). Left to self-determination, it was doomed to fail.

7. *The Issue of Public Trust*

The overall management of the COVID-19 pandemic has raised deep concerns on the ability of governments to face and counter such an unprecedented emergency. At the end of the day, the only substantive remedies were those of the past centuries against the plague and deadly fevers: lockdowns and quarantine. The transfer of all substantive powers to the central government, the ancillary role of Parliaments, widespread deference of the judiciary towards the decision of the public authorities, a substantial suspension of constitutional rights (in particular of circulation and assembly), have determined a significant and widespread mistrust by citizens towards decision-makers. In a democratic system, the promotion of public goals passes necessarily through widespread compliance with the rules introduced. Tracing apps were outside this picture and were seen as only a further burden on an already significantly impaired way-of-life. Furthermore, it is worth reflecting on the fact, registered by many pollsters, that people had shown more confidence in the idea that proximity data were collected by Google and Apple—pursuant to the decentralized model—than by the governments, under the original centralized model. This is not only telling of the distrust of governments, but also of the disregard for the strong commercial reasons behind the move of Google and Apple, which would be silly to regard as a purely altruistic act.

8. *Some Lessons for the Future*

a) The GDPR obstructs—formally and substantially—most policies, whether digital or organizational, to contrast this and future pandemics and to unlock the potential of scientific research. Either public health is put in the same special regime that already covers police and criminal investigations (see Directives 680 and 681/2016) or it will risk succumbing to the 'fundamental' right to individual privacy.

b) These concerns are quite obvious when one looks at a much more simplified issue such as that of 'vaccination passports' which would, finally, give back to European citizens one of their most cherished freedoms, that of unrestricted movement between the 27 Member States. It is no wonder that as soon as the first proposals were

disclosed to the public, national data protection authorities immediately raised strong objections based on the GDPR.

c) Coordination of health policies is still at a primitive stage in the EU. All the obstacles one has experienced over the last year in coordinating responses highlight the urgent need for pragmatic output policies. The economic and social cost that the whole of Europe is paying for a piecemeal approach, risk to broaden disaffection towards the EU.

d) In this perspective, eHealth services (surely among the best and trustworthy in the world) should become one of the main short-term goals, together with economic recovery.

e) Finally, the rise and fall of tracing apps should make us wary of the daily prophecies of the Big Data superpowers. Never, in the past, has so much information been collected throughout the world, from millions and millions of cases, concerning an illness. However, at the end of the day, the battle will be won not because some algorithm has provided us with a predictive analytic solution, but by brick-and-mortar medical research, based on trial-and-error, statistical samples of the population, laboratory and on-the-field experimentation. Fighting a pandemic is nowhere near guessing the 'sentiment' of social media goers and profiling consumer habits.

References

Ayres I, Romano A., Sotis C., *How to make COVID-19 contact tracing appswork: insights from behavioral economics*, 2020. Available at SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3689805>

Bonsall D, Parker M et al., *Sustainable containment of COVID-19 using smartphones in China: scientific and ethical underpinnings for implementation of similar approaches in other settings*, 2020. <https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Policy%20forum%20-%20COVID-19%20containment%20by%20herd%20protection.pdf>

Cho H, Ippolito S et al., *Contact tracing mobile apps for COVID-19: privacy considerations and related trade-offs*, <https://arxiv.org/abs/2003.11511>

Della Morte G, *Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo italiano*, in *Diritti umani dir int* 14(2), 2020, pp. 303–336.

Du L., Wang M., *Chinese CoViD-19 epidemic prevention and controlmeasures: a brief review,* in *Biolaw J.* 2020, <https://doi.org/10.15168/2284-4503-20201S>

European Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, 2020a. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29>

European Commission, Recommendation on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data, 2020b. <https://op.europa.eu/it/publication-detail/-/publication/1e8b1520-7e0c-11ea-aea8-01aa75ed71a1/language-en>

European Commission, *Proposal for a EU Regulation on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate)*, 2021a. <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1181>

European Commission, Proposal for a EU Regulation on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to third-country nationals legally staying or legally residing in the territories of Member States during the COVID-19 pandemic (Digital Green Certificate), 2021b. <https://www.europeansources.info/record/proposal-for-a-regulation-on-a-framework-for-the-issuance-verification-and-acceptanceof-interoperable-certificates-on-vaccination-testing-and-recovery-to-third-country-nationals-legally-staying-or>

European Data Protection Board, Guidance 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 2020a. <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf>

European Data Protection Board, Guidance n. 3/2020 on the processing of health data for the purpose of scientific research in the context of the Covid-19 outbreak, 2020b. <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf>

European Parliament, Resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences, 2020. <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.html>

Ferretti L., Wymant C. et al, *Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing*, in *Science* vol. 368(6491), eabb6936, 2020.

Findlay M, Remolina N., *Regulating personal data usage in Covid-19 control conditions*. SMU Centre for AI & Data Governance Research Paper No. 2020/04, 2020.

Garante per la protezione dei dati personali, Press Communiqué 1-3-2021 (doc. web 9550331), *No a 'pass vaccinali' per accedere a locali o fruire di servizi senza una legge nazionale*, 2021. <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9550331>

Geddie J., Aravindan A., *Singapore plans wearable virus-tracing device for all*, *Reuters*, 2020. <https://www.reuters.com/article/us-health-coronavirus-singapore-tech/singapore-planswearable-virus-tracing-device-for-all-idUSKBN23C0FO>

Greenleaf G., Kemp K., *Australia's 'COVIDSafe App': an experiment in surveillance, trust and law*. University of New SouthWales Law Research Series 999, 2020. Available at SSRN <https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3589317_code57970.pdf?abstractid=3589317&mirid=1>

Greenleaf G., Kemp K., *Australia's COVIDSafe experiment, phase III: legislation for trust in contact tracing*. UNSW Law Research, 2020. Available at SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3601730>

Gyooho L., *Legislative and administrative responses to COVID-19 virus in the Republic of Corea*, 2020. Available at SSRN <https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3587595_code1390660.pdf?abstractid=3587595&mirid=1https://dx.doi.org/10.2139/ssrn.3587595>

Hipgrave D., *Communicable disease control in China: from Mao to now*, in *J Glob Health*, vol. 1(2), pp. 224–238, 2011.

Holmes A., *Singapore is using a high-tech surveillance app to track the coronavirus, keeping schools and businesses open. Here's how it works*. Business Insider, 24 Mar 2020.

Istituto Superiore di Sanità, Rapporto ISS-Covid 19 n. 59/2020, Supporto digitale al tracciamento dei contatti (contact tracing) in pandemia: considerazioni di etica e di governance, 2020. <https://www.

iss.it/rapporti-covid-19/-/asset_publisher/btw1J82wtYzH/content/rapporto-iss-covid-19-v.-59-2020-supporto-digitale-al-tracciamento-dei-contatti-contact-tracing-in-pandemia-considerazioni-di-etica-e-di-governance.-versione-del-17-settembre-2020>

Kritikos M., *Ten technologies to fight coronavirus*. EPRS, Brussels, 2020.

Kuner C., *Data crossing borders: data sharing and protection in times of Coronavirus*, in VerfBlog, 15 Apr 2020.

Liu W. et al, *Response to the COVID-19 epidemic: the Chinese experience and implications for other countries*, in *Int J Environ Res Public Health* vol. 17, p. 2304, 2020.

Renda A., Castro R., *Towards stronger EU governance of health threats after the Covid-19 pandemic*, in *Eur J Risk Regul* vol. 11(2), pp. 273–282, 2020.

Resta G., *Data and Territory. The impact of the "local" in the regulation of digital technologies and algorithmic decision-making*, in *Essays in Honour of Mads Andenas*, forthcoming.

Savona M., *The saga of the Covid-19 tracing apps: what lessons for data governance?*. SPRU working paper series, n. 10/2020, 2020. Available at SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3645073>

Sharon T., *Blind-sided by privacy? Digital contact tracing, the Google/Apple API and big tech's newfound role as global health policy makers*, in *Ethics Inf Technol* vol. 18, pp. 1–13, 2020. <https://doi.org/10.1007/s10676-020-09547-x>

Tian H et al (2020) An investigation of transmission control measures during the first 50 days of the Covid-19 epidemic in China. Science 368(6491):638–642

Wang Z (2017) Systematic government access to private-sector data in China. In: Cate F, Dempsey J (eds) Bulk collection. Oxford University Press, Oxford

Wendehorst C., *Covid-19 apps and data protection*, in Hondius E. et al (eds) *Coronavirus and the law in Europe*. Intersentia, 2020. <https://www.comparativecovidlaw.it/2020/09/02/covid-19-appsand-data-protection>

Whitelaw S et al., *Applications of digital technology in Covid-19 pandemic planning and response*, in *Lancet Digit Health* vol. 2(8), pp. 435–440, 2020.

World Health Organisation, Contact tracing in the context of COVID-19 (Interim Guidance), 2020. <https://apps.who.int/iris/handle/10665/332049>

Xu T.et al., *China's practice to prevent and controlCOVID-19 in the context of large population movement*, in *Infect Dis Poverty* vol. 9(115), pp. 1–14, 2020.

Zastrow M., *Coronavirus contact-tracing apps: can they slow the spread of COVID-19?*, in *Nature*, 2020. <https://doi.org/10.1038/d41586-020-01514-2>

Zhang L., *Measures to control infectious diseases under Chinese law*, 2020. <https://blogs.loc.gov/law/2020/01/falqs-measures-to-control-infectious-diseases-under-chinese-law>

Zhao Q. et al., *On the accuracy of measured proximity of bluetooth-based contact tracing apps*, in Park N. et al (eds) *Security and privacy in communication networks*. Springer, Cham, p. 49, 2020.

Giorgio Resta

Towards a unified regime of data-rights?

Abstract: This paper provides a comparative introduction to the debate on data ownership, by distinguishing personal and non personal data.

1. *The debate on data rights from a comparative perspective*

At the outset, I would like to express my gratitude to the organizers of this event, and namely to Frau Dr. Tereza Pertot and to Prof. Dr. Martin Schmidt-Kessel. Not only it is a great pleasure to be back in the wonderful town of Bayreuth, but it is also a great honor for me to be invited to provide some concluding remarks at the end of such a rich and thought-provoking conference. This is, however, an uneasy task.

The papers presented by the panelists, as well as the discussions held in these two-days have touched upon some of the most controversial and neuralgic nodes of the legal infrastructure of the data economy. The organizers opted for a holistic approach: instead of focusing on specific areas or topics (such as data protection, or algorithmic decision-making), the conference was aimed at providing a general overview of the existing data rights and related regimes (see the introductory remarks by *Tereza Pertot*). This has created serious challenges for many panelists, who were confronted with the task of developing concepts and categories capable of being applied transversally to various legal relationships, having data as their main reference point. It is still difficult to judge whether this is a feasible approach which can always lead to satisfactory solutions, but there is no doubt that the comprehensiveness and the systematic character of the analysis are two of the qualities that distinguish this collection from the existing literature on the field. Given the wide range of issues and topics dealt with by the several contributors, it would be impossible for the author of these pages to focus specifically on each chapter of the book. Rather, I will try to elucidate some of the most important themes that came out of the discussion.

Let me start by a comparative remark. I think that it is not an

* This article was first published in T. Pertot (ed.), *Rechte an Daten*, Mohhr-Siebek2020, pp. 231-248.

overstatement to say that the whole debate on data ownership is – to recall a similar observation made with regard to the principle of human dignity – "like *Sauerkraut,* not exclusively German, but a German speciality"[1].

By this I mean two different things. On the one hand, the elegance of the arguments and the sophistication of the analysis, which have been achieved by German scholars in this field, is unbridged elsewhere. On the other hand, the attention attracted by such a debate both at a scholarly and at a political level – it is reported that even *Bundeskanzlerin* Merkel, in a speech given at the 49th World Economic Forum, has explicitly referred to data ownership as an issue to be clarified[2] – has no comparison in other countries. This sounds somehow paradoxical if one consider, for instance, that the problems related to the appropriation of information had been extensively analyzed in France already in the 80's[3] as well as by Italian scholars in the 90's[4]. Despite such premises, it can be hardly denied that the contribution of French or Italian authors to the contemporary debate on data-property is on the whole negligible compared to the German one. How can such a fascination for the issue of data ownership be explained?

Undoubtedly, the development of the German high-tech industry, and in particular the application of big data and smart devices in the car manufacturing sector, might have been a leading force (see for some useful insights the contribution by *Thomas Hoeren*) [5]. I suspect, however, that similar to what happened at the end of the 19th century with regard to

[1] See, in the different context of the notion of dignity, U. Wessels, *Genetic Engineering and Ethics in Germany,* in A. Dyson – J. Harris, eds., *Ethics and Biotechnology,* London, 1994, p. 237.

[2] The text of the speech can be accessed at the following address: <https://www.bundesregierung.de/breg-en/news/speech-by-federal-chancellor-angela-merkel-at-the-49th-world-economic-forum-annual-meeting-in-davos-on-23-january-2019-1574188>.

[3] P. Catala, Ébauche d›une théorie juridique de l›information, *D.,* 1984, chron., p. 97; Id., *Le marché de l'information: aspects juridiques, Petites Affiches,* 124, 1995, p. 5; Chamoux, *L'appropriation de l'information*, Paris, 1986; E. Mackaay, *La possession paisible des idées: toute information doit-elle faire l'objet d'un droit de propriété?*, *Droit de l'informatique*, 1986, 2, p. 78; N. Mallet-Pujol, *Appropriation de l'information: l'éternelle chimère, D.,* 1997, p. 330.

[4] P. Perlingieri, *L'informazione come bene giuridico*, *Rassegna dir. civ.,* 1990, p. 326; V. Zeno-Zencovich, *Informazione (profili civilistici), Dig. Disc. priv., sez. civ.,* IX, Torino, 1993, p. 823; Id., *Sull'informazione come bene (e sul metodo del dibattito giuridico), Riv. crit. dir. priv.,* 1999, p. 485.

[5] G. Seiberth – W. Gründinger, *Data-driven business models in connected cars, mobility services & beyond,* BVDW Research, No. 01/18, April 2018 (<https://www.bvdw.org/fileadmin/user_upload/20180509_bvdw_accenture_studie_datadrivenbusinessmodels.pdf>).

personality rights, among the reasons behind the "explosion" of the debate on data ownership is the problematic interaction between the peculiar architecture of the German law of torts and the "physicalist" approach to the law of property. The absence of a general clause such as the French (or even the Italian) one in § 823 I *BGB*[6] seems to work as a sort of institutional constraint, which naturally leads German scholars to vest new properties in terms of absolute rights; from this point of view, the resort to the idea of "data ownership" would be a rational solution to obtain tortious protection (as well as injunctive relief under § 1004 *BGB*) for the integrity of datasets against violations by third parties[7]. However, the narrow scope of both the notion of "thing" (§ 90 *BGB*) and "ownership" (§ 903 *BGB*) pushes in the opposite direction and creates an inherent tension with the need to fill the gaps created by the law of torts. A similar tension is absent in the French legal system, which can count not only on an inherently wider law of torts (Art. 1382 *code civil*), but also on a more flexible notion of ownership, which is sometimes held to apply to incorporeal objects as well[8].

As a matter of fact, this is exactly what happened one century ago with regard to name and image: French courts succeeded to grant immediate relief to the victims of unlawful interference with personality on the basis of the general clause of tort (Art. 1382 *code civil*), occasionally enriched by strategic references to the idea of *propriété du nom ou de l'image*[9], whereas the German scholars, starting from a much more rigid institutional setting, provided the theoretical infrastructure capable of justifying the protection of the same interests, on the basis of the idea of *Individualrechte*[10]. Not

[6] See on this point G. Wagner, *Comparative Tort Law,* in *The Oxford Hanbook of Comparative Law,* edited by M. Reimann – R. Zimmermann, Oxford, 2019, 994 et seq., at 1004-1005.

[7] For a similar remark see J. Drexl, *Designing Competitive Markets for Industrial Data. Between Propertisation and Access, JIPITEC,* 8, 2017, p. 257 et seq., 271; see also M. Amstutz, *Dateneigentum. Funktion und Form, AcP,* 218, 2018, 439, pp. 472-473.

[8] See Y. Emerich, *Droit commun des biens: perspective transsystémique,* Montréal, 2017, 261 et seq.; S. van Erp – B. Akkermans (eds.), *Cases, Materials and Text on Property Law,* Oxford – Portland, 2012, p. 379; from an historical and comparative perspective see in particular A. Candian, *Propriété,* in A. Candian – A. Gambaro – B. Pozzo (eds.), *Property — Propriété — Eigentum. Corso di diritto privato comparato*, Padova, 1992, 187 et seq.; A. Gambaro, *Proprietà in diritto comparato,* in *Dig. IV,* sez. civ., XV, Torino, 1997, 502 et seq.

[9] For an historical and comparative analysis of the French and the German experience, see G. Resta, *Autonomia privata e diritti della personalità,* Napoli, 2005, 28-120.

[10] The notion of *Individualrechte* was mainly developed by K. Gareis, *Das juristische Wesen der Autorrechte, sowie des Firmen- und Markenschutzes,* in *Archiv für Theorie und Praxis des Allgemeinen und Deutschen Handels- und Wechselrechts,* 1877, p. 185; Id.,

too differently, the recognition of an absolute right to the 'producer' of machine-readable information might also be regarded as an instinctive answer to the gaps of protection created by the municipal law of torts.

If this explanation has some merit, then the question arises whether the whole debate on data ownership would lose its meaning and appeal, once detached from the German legal and institutional framework and transposed into a different context. The answer, in my opinion, is a negative one, and this is for the elementary reason that, even leaving aside the specific proposal aimed at the recognition of a new exclusive right on raw data, still the reality of a data-driven society is the source of a whole gamut of practical issues, which the legal system, sooner or later, will be called upon to answer. Therefore, a decade of intense confrontation with the legal status of (personal and) non-personal data has not been spent in vain. It provides a theoretical framework, which might be extremely helpful – for *any* jurist, working in *any* legal system – to identify the emerging issues, relate them to the existing dogmatic categories and suggest possible solutions on the basis of the legal provisions actually in force.

The contributions collected in this book – written by German, Austrian, and Italian scholars – faithfully mirror the variety and complexity of the questions raised by data processing and data flow, as well as the usefulness of a horizontal perspective. Indeed, the assumption shared by most contributors is that today all types of data have become extremely valuable and can accomplish several functions. For instance, as explained by various authors and in particular by *Andreas Sattler* and *Thomas Riehm* in this collection[11], data may be traded as currency (data as consideration), may be used to improve commercial services offered on the market (AI, self-driving cars, domotics); may be collected with the aim of 'personalizing' the conditions of the contractual relationship (credit scoring; personalized price) [12].

Die Privatrechtssphären im modernen Kulturstaate, insbesondere im Deutschen Reiche, in *Zeitschrift für Gesetzgebung und Praxis auf dem Gebiete des Deutschen öffentlichen Rechtes,* 1877, p. 137. On this see the path-breaking analysis by D. Klippel, *Historische Wurzeln und Funktionen von Immaterialgüter- und Persönlichkeitsrechte im 19. Jahrhundert*, in *Zeitschrift für neuere Rechtsgeschichte,* 1982, p. 132.

[11] See also N. Helberger – F.Z. Borgesius – A. Reyna, *The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law, Common Market L. Rev.,* vol. 54, 2017, 1427, 1445.

[12] See the special issue of the *University of Chicago L. Rev.,* v. 86 (2019), devoted to the "personalization" of the law. See in particular A.J. Casey – A. Niblett, *A Framework for the New Personalization of the Law,* p. 333 et seq.

2. *The increasing commodification of data in a recent controversy*

It is worth noting that the most controversial legal issues concerning access to data are not strictly limited to the fields in which the phenomenon of commodification is at its peak, and namely those of machine-generated data, or consumer-related data traded by data-brokers. Even with regard to the information having the most intimate dimension, market exchanges have achieved a degree, which was hardly imaginable just a few years ago. As a result, typically proprietary and contractual issues have arisen even in those fields, which were once considered the domain of inalienable personality rights, such as health-related and genetic data.

Let me briefly recall a recent Italian case, which is paradigmatic from this point of view[13]. The case deals with the assignment, in the framework of bankruptcy proceedings, of a genetic biobank, consisting of human biological materials, demographic, epidemiological, medical and genetic data. In 2000, a public-private partnership was created with the aim of carrying out an important research project in population genetics. To this aim, a wide array of biological samples from about 11.700 voluntary donors living in Sardinia – a cluster characterised by a high degree of genetic homogeneity due to the geographic isolation and other historical factors – was collected. Owner of the biobank was the corporation SharDna (a limited liability company). In 2009, the majority shareholder sold its shares to Fondazione San Raffaele, a major Italian research and medical institution. Due to a severe financial crisis exploded in 2011, bankruptcy proceedings were opened and the Fondazione was forced to start a procedure of arrangement with creditors ("concordato preventivo"). In the framework of this procedure, the SharDna company was the object of a bargain sale by the bankruptcy court of Milan in 2012. It was purchased by the UK biotechnology company "Tiziana Life Sciences Plc" for 258.000 Euros and subsequently assigned to "Longevia genomics Srl". Following the alienation, several complaints were lodged before the Data Protection Authority by some data subjects. The Data Protection Authority ordered the blocking of the processing, on the basis of the argument that the assignee had to obtain a new consent by the persons

[13] For a more detailed analysis see C. Piciocchi – L. Ducato – L. Martinelli *et al., Legal issues in governing genetic biobanks: the Italian framework as a case study for the implications for citizen's health through public-private initiatives*, in *Journ. Community Genetics* vol. 9, 177 (2018), p. 181.

involved[14]. Longevia genomics appealed the order before ordinary courts and the Tribunal of Cagliari reversed[15]. It held that the simple change in the identity of the data controller does not deprive the original consent of its validity, as far as the aims of the processing remain unchanged. Therefore, the court refused to hold that consent was expressed *intuitu personae* – as it is generally assumed in the field of personality rights – and supported the idea that biological samples and related data are not unlike other assets for the aims of bankruptcy proceedings. *Mutatis mutandis,* the solution is not too different from the one sponsored by US scholars with regard to the right of publicity[16].

This controversy is particularly interesting, because it raises a set of legal issues, which are of critical importance for the definition of a coherent system of rules and principles on data processing.

The first issue concerns the notion of data. As it is well known, no general definition of "data" is to be found in European legal sources. "Personal data" are defined in Regulation (EU) 2016/679 as "any information relating to an identified or identifiable natural person ('data subject')". However, beyond this field, one would look in vain for less sector-specific definitions Indeed, Art. 3, point (1), Regulation (EU) 2018/1807, on a framework for the free flow of non-personal data in the European Union, tautologically defines "data" as "data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679".

We are frequently reminded – and see in this volume the contribution by *Herbert Zech* – about the need to distinguish, within the notion of "data", among three different layers[17]: *a*) the semantic level (data as information encoded in signs); *b*) the syntactic level (data as signs); *c*) the structural level (physical structures embodying data).

It deserves to be emphasized that the law may adopt simultaneously one or more of such meanings. For instance, the law of data protection starts from a semantic notion of data (Art. 4 Regulation 2016/679). In copyright law, by contrast, the syntactic level is prevailing (see § 72 UrhG), and this also the stance taken by the the proposals aimed at the recognition of new

[14] Data Prot. Auth., 6-10-2016, doc. web n. 5508051.

[15] Court of Cagliari, 18-5-2017, unpublished, available in the database *Pluris*.

[16] M.B. Jacoby – D.L. Zimmerman, *Foreclosing of Fame: Exploring the Uncharted Boundaries of the Right of Publicity*, in *N.Y.U.L. Rev.* vol. 77, 1322, 2002; M.B. Jacoby, *Auctioning Kim Basinger: The Imminent Collision of Bankruptcy and the 'Right of Publicity',* in *Norton Bankr. L. Adviser* vol. 1, 1, 2001.

[17] See also J. Drexl, *Designing Competitive Markets for Industrial Data. Between Propertisation and Access* 263.

exclusive data right (see the contribution by *Franz Hofmann*). Similarly, in Art. 1 (*b*) of the COE Convention on Cybercrime, "computer data" are defined as "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function". Furthermore, the choice for the right level of analysis might result controversial within the same part of the law. A good example is offered by human biological material, where it is highly debated whether a bodily sample may be regarded as "personal data" [18]. If the emphasis is on the information that is encoded in the sample, the answer may be affirmative; if, by contrast, the emphasis is on the material dimension of the sample, then it should be regarded only as a detached body part and not as personal data. As a matter of fact, some courts, data protection authorities and scholars endorsed the former solution[19], whereas other authorities and scholars the latter[20]. The consequences are of primary importance: if human biological materials are to be regarded as information, then data protection law will be applicable to all operations involving the collection, storage, and use of such materials; otherwise it will not.

The second issue raised by the SharDna case concerns the proprietary dimension of the collection. The Italian Data Protection Authority resisted a proprietary assessment of the biobank. However, it cannot be ignored that researchers, institutions and biotech firms tend to regard collections of DNA samples and related data as valuable assets, capable of attracting increasing flows of investments[21]. This is also the terminology constantly adopted in most Material Transfer Agreements as well as in some official documents[22]. It is commonly assumed that a genetic database might be

[18] On this see L. Bygrave, *The Body as Data? Biobank Regulation via the 'Back Door' of Data Protection Law*, *Law, Innovation and Technology,* 2, 2010, 1, pp. 6-20; W.G. Urgessa, *The Feasibility of Apllying EU Data Protection Law to Biological Materials: Challenging 'Data' as Exclusively Informational*, in *JIPITEC* vol. 7, 96, 2016.

[19] See for instance Eur. Ct. H. Rights, 8-12-2008, App. n. 30562/04 e 30566/04, *Marper v. UK*.

[20] Art. 29 Data Protection Working Party, Opinion n. 4/2007, *on the concept of personal data*: "human tissue samples (like a blood sample) are themselves sources out of which biometric data are extracted, but they are not biometric data themselves (as for instance a pattern for fingerprints is biometric data, but the finger itself is not). Therefore the extraction of information from the samples is collection of personal data, to which the rules of the Directive apply".

[21] C. Bobtcheff – C. Haritchabalet, *Economic Modeling and Valorization of Biobanks,* in X. Bioy, ed., *Public Regulation of Tumor Banks,* Heidelberg – New York, 2018, p. 63 ss.; A. Tupasela, *Data-Sharing Politics and the Logics of Competition in Biobanking,* in V. Pavone – J. Goven, eds., *Bioeconomies,* Heidelberg-New York, 2017, p. 187.

[22] L. Izac, *Commercialization Through the Use of Private Law Contracts,* in X. Bioy, ed.,

protected on the basis of the *sui generis* right introduced by Directive 96/6/EC[23]. But what about the single samples and data stored in the biobank? [24] Should the patients be regarded as owners of such properties and what kind of remedies could be awarded in the event of destruction or unlawful exploitation of the biological materials and data (f.i. for commercial purposes, as in the famous *Moore* case[25])? And what about the institution responsible for the biobank: can the model of trust – frequently referred to in the field of data rights, as detailed in the contribution by *Wendehorst*, *Schwamberger* and *Grinzinger* – be meaningfully employed also in this case?[26]

The third issue is related to contractual data flow. Starting from the assumption that biological materials and data are both useful and valuable, one might wonder whether the prohibition of financial gains, enshrined in Art. 3 of the European Charter of Fundamental Rights, might be invoked to prevent any contractual arrangement aimed at providing specific forms of benefit sharing[27]. Being this the case, DNA samples and data would be subjected to a regime of pure market-inalienability, with the consequence that the unilateral and gratuitous consent would be the only instrument of disposition legally conceivable. The question is similar to the one intensively discussed with regard to the supply of digital content on which I will be come back later.

3. *The peculiarity of personal data*

More generally, we are reminded by this controversy of the unique features of personal data. Therefore, one might seriously doubt whether a unified approach, in the sense of a general theory of data rights, would

Public Regulation of Tumor Banks, 137 et seq.

[23] L. Bygrave, *The Data Difficulty in Database Protection,* University of Oslo Faculty of Law Legal Studies Research Series N. 2012-18, 8.

[24] J.M. Rumbold – B.K. Pierscionek, *A critique of the regulation of data science in healthcare research in the European Union*, in *BMC Medical Ethics* vol. 18, 27 (2017).

[25] *Moore v. The Regents of the University of California*, 793 P.2d 479 (Cal. 1990), cert. denied, 111 S. Ct. 1388 (1991).

[26] See already D.E. Winickoff – R.N. Winickoff, *The charitable trust as a model for genomic biobanks*, in *New Engl. J. Med.* 349, 2003, 1180–1184.

[27] See F. Bellivier – C. Noiville, *Biological Sample Collection in the Era of Genomic Medicine: A New Example of a Public Commons?,* in X. Bioy, ed., *Public Regulation of Tumor Banks,* 211, 220.

be feasible or even desirable (see the contribution by *Dianora Poletti*). Various contributions have convincingly explained the reasons why two of the main pillars of a private law regime of data, namely the system of original allocation and that of voluntary transfer, would lead to different solutions as applied to personal and non-personal data (on this see *Hoeren, Hofmann, De Cristofaro, Perlingieri*).

As regards the original allocation, it has been long debated whether data could be the object of property rights, having the same structure as traditional intellectual property rights. This proposal has not been limited to non-personal data: some authors have tried to argue that also as regards personal data, the right to control guaranteed by data protection law could be conveniently framed in terms of ownership and not simply as a pure defensive-right (*Abwehrrecht*) [28].

However, this proposal has been rejected – more univocally than with regard to non-personal data – by the majority of the scholars, and this for good reasons (see in this volume the remarks by *Thomas Hoeren* and *Andrea Sattler*).

Conceptually, the aim of the protection is explicitly linked to the purpose of protecting "fundamental rights and freedoms of natural persons" with regard to the processing of personal data (Art. 1 Regulation 2016/679), and not, for example, to the aim of fostering innovation and cultural production by awarding a temporary monopoly on the exploitation of intangibles (as in the case of IP rights) [29], or reducing transaction costs by making it easier to transfer the resources to people who value them most[30]. Furthermore, the inherent logic of fundamental rights implies their inclusivity (the protection is predicated on the assumption that everybody else is simultaneously protected), whereas the mean feature of ownership rights is their exclusivity (the protection is based on the assumption that nobody else could be granted similar rights to the same object of the protection)[31].

[28] See among others L.C. Ubertazzi, *Proprietà intellettuale e privacy*, *FI*, 2014, V, c. 93; A. Wandtke, Diskussion des „Warencharakters" von Daten aus persönlichkeits- und urheberrechtlicher Sicht, *Multi-Media Recht* 2017, 6; K.H. Fezer, *Data Ownershipf of the People. An Intrinsic Intellectual Property Law Sui Generis Regarding People's Behaviour-generated Informational Data, Zeitschrift Geist. Eig.,* 9, 2017, 356.

[29] See also for critical remarks on the over-extension of IP rights, A. Peukert, *Güterzuordnung und Freiheitsschutz*, in R. Hilty, T. Jaeger, V. Kitz (eds.), *Geistiges Eigentum. Herausforderung Durchsetzung*, Springer, Berlin-Heidelberg, 2008, p. 47.

[30] See in this perspective F. Easterbrook, *Cyberspace and the Law of the Horse,* in 1996 *U. Chi. Legal F.* 207 , 1996, 212.

[31] L. Ferrajoli, *Diritti fondamentali*, in Id., *Diritti fondamentali. Un dibattito teorico,*

Secondly, from the point of view of the legal regime, data protection law is centered on the idea of balance of interests and not of the absoluteness and exclusivity of the protection. As it is made clear in Recital 4 Reg. 2016/679, "[t]he right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality"; coherently, Arts. 6 and 9 provide for a long list of cases in which data processing can be carried out on a legal basis other than consent.

Thirdly, and this concerns also the second pillar, Regulation 2016/679 openly denies one of the most important incidents of ownership, and namely the power to alienate and abandon the resource. The right to data protection is made explicitly inalienable by Art. 7, sect. 3, which grants the right to withdraw consent to data processing anytime and with no consequence whatsoever. "It shall be as easy to withdraw – it is written in the last paragraph of sect. 3 – as to give consent". Furthermore, the ban on tying introduced by Art. 7, sect. 4 is another clear sign of the intent to guarantee the freedom of self-determination (which is even more strengthened whenever special categories of data under Art. 9 are involved) and hence to disregard a pure proprietary logic, such as the one implied in the US model of data protection[32].

This does not mean that data cannot be traded as currency[33]. Despite the symbolic wording of Directive 2019/770/EU, it can be hardly denied that data, as a matter of fact, are treated as consideration in a plurality of settings, from the insurance sector to electronic communications. They are at the center of a complex network of contractual relationships, which provide the institutional structure for the extraction of the value of data, as detailed by *Andreas Sattler* in this volume. However, contracts over personal data are necessarily characterized by a peculiar physionomy as well as by specific rules, aimed at balancing the reliance interest with the personal nature of the resources involved[34]. Dogmatically, the coordination between Regulation 2016/679 and Directive 2019/770 would be best achieved by assuming that the "consent" to data processing (whose legal regime has

Roma-Bari, 2008, pp. 12-15.

[32] On this point see P.M. Schwartz – K.N. Peifer, *Transatlantic Data Privacy Law,* in *Georgetown Law Journal* vol. 106, 115, 2017, pp. 143, 152.

[33] See generally C. Langhanke – M. Schmidt-Kessel, *Consumer Data as Consideration,* in *EuCML,* 2015, p. 218.

[34] See G. Resta – V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.,* 2018, 411 et seq., 433-435.

to be inferred from the GDPR) has a unilateral structure and works as a sort of *Geschäftsgrundlage* with regard to the bilateral contract (regulated by Directive 2019/770 and applicable national provisions), which is aimed at setting the conditions for the supply of digital content (on this see the detailed analysis by *Thomas Riehm* and *Giovanni De Cristofaro*) [35]. Operationally, contracts over personal data find specific constraints in the provisions of Regulation 2016/679 and namely in the principles of purpose-limitation, data minimization, as well as inherent precarity of the relationship (ensuing from the right to withdrawal under Art. 7, sect. 3). Lastly, the right to portability works as a final guarantee of the freedom to self-determination, by making it always possible to reverse the original contractual allocation and dispose of the data to the benefit of a third party or of the data subject. Once again, the position of the data controller *vis-à-vis* the data subject seems to have its closest analogue in the position of a fiduciary rather than of a new owner (see the contribution by *Wendehorst*, *Schwamberger* and *Grinzinger*). By looking at such constraints, it is easily understood why the "personality" of data may be regarded as a limit, rather than as a trigger of data trade (see the paper by *Andreas Sattler*).

4. *Data as a legal object and the plurality of legal regimes*

The peculiarity of the regulatory logic concerning personal data is also confirmed by the architecture of the legal sources. It is worth recalling, in particular, that Regulation 2018/1807 specifically concerns the free flow of non-personal data, thereby creating a double-track in the EU approach to transnational data flow.

This leads to a further, important, point. The field of personal data is intensively regulated, both at a European and at a national level, making the recourse to general private law less compelling (see on this the contribution by *Dianora Poletti*, dealing with the possible extension of the category of possession to personal data). The opposite is true with regard to non-personal data. Few legal provisions deal with the production, collection, processing and transfer of non-personal data. This makes the task of legal scholars a particularly delicate and important one. Not by chance, the most innovative and creative part of the debate concerning rights over data has

[35] See also G. Resta, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il Regolamento (UE) 2016/679,* in *Annuario del Contratto,* 2018, 127 et seq.

been focusing on this sub-sector.

The contributions collected in this volume deal with two main questions: *a*) can data be owned?; *b*) can the provisions and the conceptual categories concerning the *rights in rem* be extended to data?

5. *Exclusive rights on non-personal data?*

(*a*) The issue of data ownership has been extensively scrutinized over the last few years[36]. *De lege lata,* no exclusive right over data is deemed to exist (see in this collection *Hoeren, Hofmann* and *Sattler*). As it can be inferred by the useful taxonomy provided by *Franz Hofmann,* the allocation of rights over intangibles can be achieved through various legal techniques, having different intensity: from the indirect protection achieved by means of factual control or the law of unfair competition, to the strongest one *via* full-blown exclusive rights (*Ausschliesslichkeitsrechte*). Whereas the availability of indirect forms of protection of raw data – on the basis of contract law, or the law of trade secrets – can be hardly denied, the opposite is true as regards the recognition of a full-blown exclusive right (see *Franz Hofmann*). This would require a specific legislative intervention and could not be obtained in the shadow of the law. The principle of *numerus clausus* of exclusive rights over intangibles – which deserves to be strongly reaffirmed, despite the contemporary over-protectionist tendencies in the field of intellectual property[37] – would run against such a result. As it has been very well shown by *Alexander Peukert*, its inherent logic is different from the one relating to the *rights in rem*[38]. Given that intangibles are economically non-rivalrous, this principle is not aimed at avoiding the over-consumption of resources, but rather at preserving a democratically decided balance between spheres of liberty and spheres of property. The recognition of a new exclusive right automatically produces

[36] For an overview see J. Stender-Vorwachs – H. Steege, *Wem gehören unsere Daten? Zivilrechtliche Analyse zur Notwendigkeit eines dinglichen Eigentums an Daten, der Datenzuordnung und des Datenzugangs, NJOZ* 2018, 1361; M. Amstutz, *Dateneigentum. Funktion und Form,* 439 et seq.

[37] See A. Ohly, *Gibt es einen Numerus clausus der Immaterialgüterrecht?*, in *Festschrift für Gerhard Schricker zum 70. Geburtstag*, Beck, München, 2005, 105; G. Resta, *Nuovi beni immateriali e* numerus clausus *dei beni esclusivi,* in G. Resta, ed., *Diritti esclusivi e nuovi beni immateriali,* Milano, 2010, 3 et seq.

[38] A. Peukert, *Güterzuordnung als Rechtsprinzip,* Tübingen, 2008, 21-23, 763 et seq.

a restriction of the preexisting domain of freedom, negatively impacting upon positions such as the right to information or the right to undergo an economic activity. Therefore, what is needed is an informed assessment of costs and benefits of new property rights, one that may be achieved only by Parliaments and not by the decentralized court system[39].

(*b*) This naturally leads to the most controversial question, namely, whether the introduction of exclusive rights on machine-generated data is socially desirable. Whereas in the first stage proposals such as those advanced by *Herbert Zech*[40] have attracted much attention and had been tentatively endorsed even by the European Commission[41], in recent times the critiques raised against the prospect of a new exclusive right on data have gained traction.

Objections touch upon various aspects, as detailed in the contribution by *Franz Hofmann*. Some of them deal with technical details of the proposal, such as the objective (*what* should be protected and to what *extent*) or the subjective (*who* should benefit) scope of protection[42]. Others are more substantial and focus on the social effects of the new monopoly right. In particular, as forcefully put forth by *Josef Drexl*, the introduction of exclusive rights over intangibles is just another form of market regulation, having substantial impacts on the position of competitors, and as such it should be specifically justified and based on compelling reasons[43]. According to the standard economic analysis, intellectual property rights are aimed at correcting a market failure, which does not ensue from the overconsumption of the resource (as in the case of tangibles), but rather from its under-production. The promise of monopoly profit should trigger inventive and creative activities, which otherwise could end up not being undertaken. Therefore, the question is the following: would the benefits ensuing from the new exclusive position plausibly justify the costs deriving from the restriction of antagonistic freedoms?

[39] A. Peukert, *Güterzuordnung als Rechtsprinzip,* 730 et seq.

[40] H. Zech, *Daten als Wirtschaftsgut – Überlegungen zu einem "Recht des Datenerzeugers", CR,* 2015, 137 et seq.

[41] See European Commission's Communication, *Building a European Data Economy,* 10-1-2017, COM (2017) 9 final, 13; on this H. Zech, *Building a European Data Economy – The European Commission's Proposal for a Data Producer's Right, Zeitschrift Geist. Eig.,* 9, 2017, 317.

[42] J. Drexl, *Designing Competitive Markets for Industrial Data. Between Propertisation and Access,* 276-278.

[43] For a similar remark see J. Drexl, *Designing Competitive Markets for Industrial Data. Between Propertisation and Access,* 260 et seq.

The skepticism shown by many scholars seems justified[44]. On the one hand, despite the absence of exclusive entitlements, a particularly dynamic and innovative data industry has developed everywhere, taking advantage of the existing legal techniques (such as trade secrets) as well as of factual control (amenable to various contractual arrangements, as explained my *Markus Artz* in his oral contribution) over data[45]. On the other hand, the negative externalities arising from a supposed veto right tend to increase substantially with the development of deep learning and artificial intelligence. Access to the widest possible amount of data for purposes of analysis and aggregation is essential for the smoother workings of such technologies[46]. Therefore, any unnecessary hurdle to the free availability of data risks impeding, instead of fostering, social innovation and economic development (a similar debate involved the evaluation of Directive 96/9/EC on the legal protection of databases).

It is not by chance that the emphasis has gradually shifted from the pole of protection to the one of access. Competition law, consumer law, as well as fundamental rights have been increasingly referred to as possible bases for the recognition of special guarantees of access to data[47]. It is particularly meaningful, from this point of view, that even the European Commission seems to have abandoned the 'protectionist' perspective. In the 2018 Communication "Towards a common European data space" [48], the keyword is no more "exclusion", but rather "sharing" [49]. As a result, the main question at the center of the debate today is: how to guarantee access to data and no more how to design proprietary structures.

[44] See J. Drexl, *Designing Competitive Markets for Industrial Data. Between Propertisation and Access,* 273; W. Kerber, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, GRUR Int.*, 2016, 989-999.

[45] F. Mezzanotte, *Access to Data: The Role of Consent and the Licensing Scheme,* in S. Lohsse – R. Schulze - D. Staudenmayer (a cura di), *Trading Data in the Digital Economy: Legal Concepts and Tools*, Oxford – Baden-Baden, 2017, 159 et seqq., 167.

[46] D. Pedreschi – F. Giannotti et al., *Open the Black Box. Data-driven Explanation of Black Box Decision Systems,* in *ArXiv,* 1 (2018), 1-2.

[47] See for an overview H. Schweitzer – M. Peitz *Ein neuer europäischer Ordnungsrahmen für Datenmärkte?*, *NJW,* 2018, 275, 279-280.

[48] European Commission Communication, *Towards a common European data space,* 25-4-2018, COM (2018) 232 final.

[49] See H. Richter – P.R. Slowinski, *The Data Sharing Economy: On the Emergence of New Intermediaries*, *IIC* 2019, 4 et seq.

6. *Data as an object of possession?*

The obstacles encountered by the model of *Dateneigentum* logically bring into to the limelight the question that is at the core of this symposium, and namely: what is the proper legal-theoretical framework for the assessment and conceptualization of the contemporary practices of data handling and data trade? Can general private law, and especially the rules on real rights, offer appropriate hints for the design of an efficient regulatory system?

We have already seen that, in the field of personal data, most of the relevant issues can be satisfactorily approached and solved through the existing legal provisions and the (at least) 20 years long doctrinal and judicial confrontation with data protection. In the field of non-personal data, by contrast, the situation is much more confused and un-settled. The oral presentation by *Alberto Gambino* as well as the written contributions by *Herbert Zech* and *Thomas Hoeren* deal with an issue, which paradigmatically illustrates the types of questions that a modern law of data necessarily has to answer: may data be the object of possession? Shall the civil code provisions concerning the acquisition of possession, transfer and loss as well remedies in case of violation be applicable to data?

There are several difficulties.

First, from a formalist point of view, it cannot be overlooked that the provisions on possession (for ex. § 584 *BGB*) or more generally on property and the *rights in rem* (Art. 810 It. c. civ.), are in many civilian systems expressly limited to "things". Of course, it can even be discussed whether a "thing" is ontologically a corporeal one and therefore possession of intangibles cannot be but a constructive one (as it was stipulated in the famous English debate at the end of the 19th century) [50], or whether it can comprise incorporeal objects (as it has been sometimes argued in Austria[51] and in Italy[52], or is currently debated in China, with regard to Art. 127

[50] This debate was opened by the article by H.W. Elphinstone, *What is a Chose in Action?, Law Quart. Rev.,* 1893, 311; on this see in particular R. Sacco – R. Caterina, *Il possesso,* in *Trattato di diritto civile e commerciale* diretto da A. Cicu, F. Messineo e L. Mengoni, Milano, 2014, 126.

[51] On the basis of § 311 ABGB: on this see the contribution by Wendehorst, *Schwamberger* and *Grinzinger,* in Herausgegeben von T. Pertot, unter Mitwirkung von M. Schmidt-Kessel und F. Padovini, *Rechte an Daten*.

[52] This is, however, a stance taken only by the minority of the scholars: see A. Gambaro, *I beni*, in *Trattato di diritto civile e commerciale Cicu-Messineo,* Milano, 2012, 16 et seq.

of the new General Rules of the Civil Law entered into force in 2017[53]). However, both in Germany and in Italy, the solution adopted by the majority of scholars is against the possession of intangibles[54].

Secondly, assuming that either a broader reading, or an extension by way of analogy of such provisions is feasible, it should be demonstrated that, from a functional point of view, this is a workable solution. Indeed, the rationale upon which most of the rules on possession are designed is the material apprehension and the factual control of a tangible thing[55]. In particular, one of the main functions of the legal institution of possession is – together with its signaling function[56] – the protection of social peace (*Befriedungsfunktion*), which might be endangered if the existing relationships with things did not gain immediate protection by the law. This mechanism makes sense with regard to things that are rivalrous in consumption[57], but ends up being inherently fragile with regard to intangibles, which can be enjoyed by more than one person simultaneously. This is the reason why the various proposals aimed at recognizing some forms of possession in the field of intellectual property rights have always been met with skepticism[58]. In the end, conceptual categories and institutions which had been developed in the framework of an agricultural and industrial economy can hardly fit the needs of an information society.

Lastly, resorting to general private law categories might appear counterproductive from the broader point of view of the ongoing "europeanization" of data rights[59]. Indeed, whereas many efforts have been devoted to the creation of a digital single market, the very idea of filling the gaps through categories offered by national private law risks pushing in the opposite direction, leading to a further fragmentation of the regulatory framework. It cannot be overseen that European legal systems differ

[53] See L. Yi, *Daten als eigentumsrechtlicher oder immaterialgüterrechtlicher Gegenstand in China*, *GRUR Int.,* 2019, 238 et seq.

[54] R. Sacco – R. Caterina, *Il possesso,* 127; as regards Germany see the contribution by H. Zech, and T. Hoeren, *Datenbesitz statt Dateneigentum. Erste Ansätze zur Neuausrichtung der Diskussion um die Zuordnung von Daten, MMR,* 2019, 5.

[55] A. Gambaro, *La proprietà. Beni proprietà possesso,* in *Trattato di diritto privato* diretto da Iudica e Zatti*,* 2 ed., Milano, 2017, p. 466.

[56] See Y. Emerich, *Droit commun des biens: perspective transsystémique,* Montréal, 2017, 70.

[57] A. Peukert, *Güterzuordnung als Rechtsprinzip,* Tübingen, 2008, 213 et seq.

[58] See R. Sacco – R. Caterina, *Il possesso,* 130; V. Jänich, *Geistiges Eigentum – eine Komplementärerscheinung zum Sacheigentum?,* Tübingen, 2002, 220 et seq.

[59] H. Schweitzer – M. Peitz *Ein neuer europäischer Ordnungsrahmen für Datenmärkte?*, 275 et seq.; A. De Franceschi, ed., *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution,* Cambridge-Antwerp-Portland, 2016.

significantly in relation to some of the main pillars of the law of property, such as the material scope of the notion of "thing" (the narrower German approach contrasting with the more flexible Austrian or French one) [60], the structure and content of possession[61], the distinction between *possessio* and *detentio*[62], or the rules concerning voluntary transfer of property rights[63].

7. *National private law or European law: looking for the proper framework*

Given such a fragmentation, it seems wiser to follow a different path. Instead of taking a bottom-up perspective (from national private law to the European sources), we should rather opt for a top-down approach (from the European sources to national private law). Similarly to what happened in the field of data protection, also with regard to non-personal data, it could prove more productive to start from both the rules and the categories enshrined in the European sources and build around them a transnationally more consistent theoretical framework[64]. The contribution by *Herber Zech* is a good example in point: after having demonstrated why – under German law – the category of possession cannot be meaningfully transposed to the field of intangibles, he advocates the resort to the different notions of "access" or "control" of data, which are positively employed in the Directive (EU) 2016/943 on the protection of undisclosed know-how and business information against their unlawful acquisition, use and disclosure. Art. 2 of the Directive defines "trade secret" as any information which is secret, in the sense that it is not "generally known among or *readily accessible* to persons within the circles that normally deal with the kind of information in question", it has commercial value, and "has been subject to reasonable steps under the circumstances, by the person lawfully *in control* of the information, to keep it secret". A similar approach is followed by *Thomas Hoeren*, who also refers to the new legislation on trade secrets

[60] A. Gambaro, *I beni*, 16, 38 ss.; see also on this point the contribution by Wendehorst, Schwamberger and Grinzinger.
[61] A. Gambaro, *La proprietà. Beni proprietà possesso,* 475-477.
[62] See S. van Erp – B. Akkermans (eds.), *Cases, Materials and Text on Property Law,* 719; Y. Emerich, *Droit commun des biens: perspective transsystémique,* 62-65, 97-100.
[63] See S. van Erp – B. Akkermans (eds.), *Cases, Materials and Text on Property Law,* 787 et seq.
[64] This is an approach specifically advocated by A. Gambaro, "*Jura et leges" nel processo di edificazione di un diritto privato europeo, Europa e diritto privato,* 1998, 993-1018.

as a possible basis for the construction of an autonomous theory of "data control". Of course, this does still not provide a solution for most of the underlying issues, but at least it is a useful starting point for further work in the field.

Giorgio Resta

I dati personali oggetto del contratto
Riflessioni sul coordinamento tra la direttiva (UE) 2019/770 e il regolamento (UE) 2016/679

Sommario: 1. I dati come beni in senso giuridico – 2. Il modello "servizi contro dati" e la direttiva sulla fornitura di contenuti digitali – 3. La disciplina del consenso nel regolamento sulla protezione dei dati personali – 4. Il coordinamento tra la direttiva 2019/770 e il regolamento 2016/679 – 5. Conclusioni.

Abstract: This paper reflects on the issue of data as consideration, by providing an analytic framework aimed at reconciling Directive 2019/770 and the GDPR.

1. *I dati come beni in senso giuridico*

I dati personali, e così i dati *tout court* possiedono al giorno d'oggi un rilevante valore economico [1]. L'intero sistema dell'industria 4.0, che è tipicamente *data driven*, non può essere compreso prescindendo da tale assunto. I dati costituiscono, in particolare, un elemento essenziale di molti prodotti e servizi "smart" offerti sul mercato, possono essere la fonte di un rilevante vantaggio competitivo (come dimostrano i valori in borsa di aziende come Facebook e Google), e le applicazioni dell'intelligenza artificiale non fanno altro che rafforzare la premessa iniziale. Tuttavia, l'acquisizione di un valore economico, com'è noto, non è di per sé un presupposto condizionante rispetto alle scelte di valorazione giuridica dei beni[2].

Stabilire se un'entità, che abbia acquisto sul piano socio-economico un

* Questo articolo è stato originariamente pubblicato in *Annuario del Contratto*, 2019, pp. 125-151.

[1] V., ad es., G. Malgieri-B. Custers, *Pricing Privacy: The Right to Know the Value of Your Personal Data*, in *Computer Law & Security Review*, 34, 2018, p. 289 ss.; H. Zech, *Data as a Tradeable Commodity*, in A. De Franceschi (a cura di), *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution*, Cambridge-Antwerp-Portland, 2016, p. 51 ss.

[2] In luogo di molti v. a questo riguardo A. Gambaro, *I beni*, in *Tratt. Cicu-Messineo*, Giuffrè, 2012, spec. p. 34 ss.; M. Costantino-R. Pardolesi-G. Bellantuono, *I beni in generale*, in *Tratt. Rescigno*, VII, (2ª ed.), Utet, 2005, p. 1 ss.

apprezzabile valore di scambio, sia un bene tecnicamente appropriabile e poi, secondariamente, se sia suscettibile di costituire oggetto di contratti, aventi efficacia obbligatoria o reale, è scelta rimessa esclusivamente all'ordinamento giuridico (cfr. unicamente art. 810 c.c.).

Quanto al primo aspetto, di recente si è molto dibattuto se sia possibile riconoscere, a diritto vigente, un diritto esclusivo sui dati non personali, e segnatamente sui *machine produced data*, il quale trascenda i limiti sottesi alla tutela del costitutore di banche dati o al titolare di segreto industriale [3]. Del pari, diversi autori hanno difeso la tesi per cui dei dati personali possa predicarsi una vera e propria appartenenza di stampo proprietario [4]. *Mes data sont à moi:* così recita uno slogan coniato da un *think tank* francese di impostazione liberista vicino al partito governativo *En Marche* [5].

Su tali problemi si potrebbe dibattere a lungo, e sarebbe opportuno farlo non rimanendo limitati alla prospettiva d'indagine propria del giurista, ma integrando nell'analisi le risultanze della riflessione dei sociologi, degli economisti, dei filosofi e degli informatici. Esulando dagli scopi della presente trattazione un'analisi monografica di tale tematica, basterà limitarsi a segnalare come le obiezioni mosse nei confronti delle prospettazioni di stampo proprietario appaiono difficilmente superabili. E ciò perché il sistema europeo della tutela dei dati personali è costruito in funzione attuativa del precetto di protezione dei diritti fondamentali, e segnatamente del diritto iscritto nell'art. 8 della Carta UE. Il regolamento 2016/679/UE [6], in particolare, non è volto a riconoscere privative su beni

[3] Su questo problema v. M. Becker, *Rights in Data – Industry 4.0 and the IP Rights of the Future*, in *Zeitschrift für geistiges Eigentum*, 9, 2017, p. 253; nonché i saggi raccolti nel volume curato da S. Lohsse-R. Schulze-D. Staudenmayer, *Trading Data in the Digital Economy: Legal Concepts and Tools*, Oxford-Baden Baden, 2017, ed in particolare gli scritti di B. Hugenholtz, *Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit?*, p. 75 ss.; F. Mezzanotte, *Access to Data: The Role of Consent and the Licensing Scheme*, p.159 ss.

[4] V. Janeček, *Ownership of personal data in the Internet of Things*, in *Computer Law & Security Review*, 34, 2018, p. 1039 ss.; C. Berger, *Property Rights to Personal Data? An Exploration of Commercial Data Law*, in *Zeitschrift* für *geistiges Eigentum*, 9, 2017, p. 340 ss.; S. Gutwirth-G. González Fuster, *L'éternel retour de la propriété des données: de l'insistance d'un mot d'ordre*, in E. Degrave-C. de Terwangne-S. Dusollier (a cura di), *Law, norms and freedoms in cyberspace – Liber amicorum Yves Poullet*, Larcier, 2018, p. 117 ss.; L.C. Ubertazzi, *Proprietà intellettuale e privacy*, in *Foro it.*, 2014, V, c. 93.

[5] Di ciò riferisce J. Drexl, *Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy*, in A. De Franceschi *et al.*, *Digital Revolution: New Challenges for Law*, in corso di pubblicazione per i tipi di Beck, München.

[6] Regolamento 2016/679/UE del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati persona-

immateriali, bensì a *tutelare le persone fisiche* «con riguardo al trattamento dei dati personali» (come recita il titolo dello stesso atto normativo); e, dunque, a bilanciare l'interesse al controllo sull'utilizzazione dei propri dati personali con l'opposto interesse all'accesso e alla circolazione delle informazioni. È, invece, assente dalla prospettiva di intervento del legislatore, e più in generale del diritto europeo, l'idea di ascrivere diritti esclusivi aventi contenuto patrimoniale sui dati personali [7].

Non è invece estraneo all'impianto regolatorio sottostante l'obiettivo di conciliare la protezione degli interessi della persona con il fluido funzionamento del mercato intracomunitario delle informazioni. Perciò, piuttosto che attardarsi a ribadire gli argomenti, più volte avanzati, in grado di smentire l'assunto dei dati personali come termine di riferimento di diritti di privativa, appare più produttivo concentrarsi sui rapporti negoziali "a valle", per comprendere in che modo il suddetto contemperamento di interessi possa essere perseguito nella fase "dinamica" della circolazione dei dati personali.

In particolare, è necessario porsi tre ordini di domande: *a*) i dati personali possono costituire oggetto di un contratto?; *b*) quali sono gli effetti che siffatti accordi sono in grado di produrre?; *c*) attraverso quali regole la natura fondamentale ed inalienabile del diritto alla protezione dei dati può essere conciliata con la vincolatività degli effetti propria dello strumento contrattuale?

Il settore della protezione dei dati personali è ormai quasi integralmente disciplinato dalle fonti di diritto europeo, primario e derivato. Perciò, per rispondere ai quesiti pocanzi formulati, è necessario adottare una prospettiva multilivello, integrando l'analisi del diritto interno con il diritto sovranazionale. In particolare, è necessario soffermare l'attenzione su due diversi testi, che, sia pure da differenti prospettive, si accostano al problema della "disposizione" dei dati personali. Il primo attiene, in senso ampio, al settore della contrattazione *online* e in particolare alla tutela dei diritti dei consumatori; il secondo alla protezione dei dati personali. Si allude, rispettivamente, alla direttiva 2019/700/UE relativa alla fornitura di contenuti e servizi digitali [8], e al regolamento 2016/679/UE sulla protezione dei dati personali [9].

li, nonché alla libera circolazione di tali dati.

[7] Per una più approfondita argomentazione, mi permetto di rinviare a G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Pol. dir.*, 2019, p. 199 ss., spec. pp. 204-205.

[8] Direttiva 2019/770/UE del Parlamento Europeo e del Consiglio del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuti digitali e di servizi digitali.

[9] Regolamento 2016/679/UE del Parlamento Europeo e del Consiglio del 27 aprile 2016, cit.

2. *Il modello "servizi contro dati" e la direttiva sulla fornitura di contenuti digitali*

La direttiva 2019/770/UE sulla fornitura di contenuti e sevizi digitali si connota per un approccio dichiaratamente realistico. Essa non ignora, cioè, ed è questo uno dei suoi pregi maggiori, l'evoluzione dei rapporti di mercato e lo straordinario valore che i dati personali hanno assunto nel contesto dell'economia dell'informazione [10].

In particolare, essa muove dalla constatazione che in vari segmenti di mercato, e in particolare in presenza di mercati "a più versanti" [11], si è passati dal modello dello scambio remunerato a quello del servizio gratuito. La "zero marginal cost society", di cui scrive Rifkin [12], è una realtà ormai consolidata ed uno dei fattori su cui essa si basa è costituito proprio dal significato economico della disponibilità dei dati.

Non è certo per spirito di liberalità o per disinteressata generosità che molti servizi digitali, come la posta elettronica, l'accesso a *social network*, i servizi di *cloud*, i quali pure hanno un costo di esercizio non del tutto trascurabile, sono offerti a titolo gratuito [13]. Il sistema peraltro trascende lo stretto ambito dell'economia digitale, per interessare ormai una pluralità di rapporti: si pensi unicamente, da questo punto di vista, ai contratti di assicurazione r.c. che prevedono premi ridotti qualora l'assicurato consenta all'installazione nella propria autovettura di una "scatola nera" atta a

[10] Su questo punto, tra i molti, v. A. Metzger, *Dienst Gegen Daten: Ein Synallagmatischer Vertrag*, in *AcP*, 2016, p. 818 ss.; H. Zech, *Data as a Tradeable Commodity*, cit., p. 51 ss.; A.-A. Wandtke, Ökonomischer *Wert von Persönlichen Daten. Diskussion des 'Warencharakters' von Daten aus persönlichkeits– und urheberrechtlicehr Sicht*, in *Multimedia und Recht*, 2017, p. 6 ss.; M. Bisges, *Personendaten, Wertzuordnung und Ökonomie. Kein Vergütungsanspruch Betroffener für die Nutzung von Personendaten*, *ivi*, 2017, p. 301 ss.; C. Langhanke-M. Schmidt-Kessel, *Consumer Data as Consideration*, in *EuCML*, 2015, p. 218 ss.

[11] Il riferimento è alla ricca elaborazione della scienza economica in tema di piattaforme e *multi-sided markets:* v. oltre al celebre studio di J.C. Rochet-J. Tirole, *Platform Competition in Two Sided Markets*, in *Journal of the European Economic Association*, 1(4), 2003, p. 990, A. Hagiu-Wright, *Multi-Sided Platforms*, in *International Journal of Industrial Organization*, 43, 2015, p. 162; M. Rysman, *The Economics of Two-Sided Markets*, in *Journal of Economic Perspectives*, 23, 2009, p. 125.

[12] J. Rifkin, *The Zero Marginal Cost Society. The Internet of Things, The Collaborative Commons, And the Eclipse of Capitalism*, St. Martin's Press, 2014.

[13] In tema M. Narciso, *'Gratuitous' Digital Content Contracts in EU Consumer Law*, *Consumer Law*, in *EuCML*, 2017, p. 198 ss.

registrare tempi, modalità e condizioni di guida, oltre ad dati personali [14]. Nonostante l'apparente gratuità, tutti questi servizi sono remunerati adeguatamente – sebbene in maniera opaca – attraverso il flusso dei dati personali connesso alla singola transizione o alla serie di transazioni rese possibili dall'attivazione del servizio. Di qui l'esigenza di sottoporre tali rapporti ad una disciplina non divergente da quella ordinaria, in particolare per quanto concerne i profili di tutela del consumatore.

Questo è il senso, indipendentemente da alcune alchimie lessicali, alle quali si farà cenno a breve, del primo comma dell'art. 3, ove si stabilisce l'applicabilità della direttiva 2019/770/UE non soltanto ai contratti in cui il consumatore, in cambio del contenuto o servizio digitale fornito dal fornitore, corrisponde o si impegna a corrispondere un prezzo, ma anche ai contratti tramite i quali «l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dall'operatore economico ai fini della fornitura del contenuto digitale o del sevizio digitale a norma della presente direttiva o per consentire l'assolvimento degli obblighi di legge cui è soggetto l'operatore economico e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti».

Il ragionamento di *policy* che è sotteso alla scelta di estendere l'applicabilità della direttiva medesima ai rapporti "servizi contro dati" è esplicitato nel considerando 24. Converrà riprodurne per interno il testo:

«La fornitura di contenuti digitali o di servizi digitali spesso prevede che, quando non paga un prezzo, il consumatore fornisca dati personali all'operatore economico. Tali modelli commerciali sono utilizzati in diverse forme in una parte considerevole del mercato. Oltre a riconoscere appieno che la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce, la presente direttiva dovrebbe garantire che i consumatori abbiano diritto a rimedi contrattuali, nell'ambito di tali modelli commerciali. La presente direttiva dovrebbe pertanto applicarsi ai contratti in cui l'operatore economico fornisce, o si impegna a fornire, contenuto digitale o servizi digitali al consumatore e in cui il consumatore fornisce, o si impegna a frnire, dati personali. I dati personali potrebbero essere forniti all'operatore economico al momento

[14] Sul punto, anche per ulteriori riferimenti, A. De Franceschi, *La circolazione dei dati personali nella proposta di direttiva UE sulla fornitura di contenuti digitali*, in A. Mantelero-D. Poletti (a cura di), *Regolare la tecnologia: il regolamento UE 2016/679 e la protezione dei dati personali*, Pisa University Press, 2018, p. 203 ss., 204.

della conculsione del contratto o successivamente, ad esempio nel momento in cui il consumatore acconsente a che l'operatore economico utilizzi gli eventuali dati personali caricati o creati dal consumatore utilizzando il contenuto digitale o il servizio digitale. Il diritto dell'Unione in materia di protezione di dati personali prevede un elenco esaustivo di fondamenti giuridici per il trattamento lecito dei dati personali. La presente direttiva dovrebbe applicarsi ai contratti in cui il consumatore fonirsce, o si impegna a fornire, dati personali all'operatore economico. Ad esempio, la presente direttiva dovrebbe applicarsi nel caso in cui il nome e l'indirizzo email forniti da un consumatore al momento della creazione di un account sui social media vengano utilizzati per scopi diversi dalla mera fornitura di contenuti digitali o servizi digitali o non conformi agli obblighi di legge. La presente direttiva dovrebbe altresì applicarsi nel caso in cui il consumatore acconsenta a che il materiale che caricherà e che contiene dati personali, come fotografie o post, sia trattato a fini commerciali dall'operatore economico. Gli Stati membri dovrebbero tuttavia mantenere la facoltà di decidere in merito al soddisfacimento dei requisiti in materia di formazione, esistenza e validità di un contratto a norma del diritto nazionale».

Si deve notare che la versione originaria della Proposta di direttiva licenziata dalla Commissione prediligeva una diversa formulazione [15]. In particolare, l'art. 3, c. 1, configurava espressamente i dati personali come «controprestazione non pecuniaria» atta a sorreggere sul piano causale la fornitura di servizi o contenuti digitali [16]; e dava atto, nel considerando 13 che nell'economia digitale, «gli operatori del mercato tendono spesso e sempre più a considerare le informazioni sulle persone fisiche beni di valore comparabile al denaro. I contenuti digitali sono spesso forniti non a fronte di un corrispettivo in denaro ma di una controprestazione non pecuniaria, vale a dire consentendo l'accesso a dati personali o altri dati».

L'espressa qualificazione dei dati personali come "controprestazione" aveva dato luogo ad equivoci ed obiezioni, che si trovano espressi con particolare forza argomentativa nell'apposito parere reso dallo

[15] Proposta di direttiva del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, COM(2015)634 final. Per una prima introduzione alla proposta v. G. Spindler, *Verträge über digitale Inhalte – Anwendungsbereich und Ansätze – Vorschlag der EU-Kommission zu einer Richtlinie über Verträge zur Bereitstellung digitaler Inhalte*, in *MMR*, 2016, p. 147 ss.

[16] Ivi si stabiliva, in particolare, che la direttiva si applica ai «contratti in cui il fornitore fornisce contenuto digitale al consumatore, o si impegna a farlo, e in cambio del quale il consumatore corrisponde un prezzo oppure fornisce attivamente una controprestazione non pecuniaria sotto forma di dati personali o di qualsiasi altro dato».

European Data Protection Supervisor [17]. Tale documento ricorda che il regolamento 2016/ 679/UE «mette in guardia contro nuove disposizioni che introducono il concetto che le persone possono pagare con i propri dati, nello stesso modo in cui pagano in denaro. I diritti fondamentali, come il diritto alla protezione dei dati personali, non possono essere ridotti a semplici interessi dei consumatori e i dati personali non possono essere considerati una mera merce» [18]. Da queste valutazioni traspare non soltanto un diverso apprezzamento delle implicazioni sistematiche dell'art. 3 della proposta, ma il conflitto tra due antitetici modelli di lettura del diritto alla protezione dei dati: l'uno, riflesso nella versione originaria della proposta, improntato ad una lettura se non patrimonialistica quanto meno pragmatica del fenomeno della circolazione dei dati; l'altro, scolpito nelle parole del garante europeo, orientato in chiave prettamente personalistica. Secondo quest'ultima prospettiva, i dati non potrebbero essere equiparati ad una merce e come tali non dovrebbero essere suscettibili di integrare il sinallagma contrattuale.

Ad osservare le modifiche apportate nel testo finale della direttiva, si potrebbe essere indotti a pensare che quest'ultima lettura abbia avuto la meglio. Da un lato, infatti, si è abbandonata l'espressa qualificazione dei dati come «controprestazione non pecuniaria»; dall'altro, si è espressamente ribadito nel considerando 14 che i dati personali «non possono essere considerati una merce».

Tuttavia, mentre non si può che esprimere soddisfazione per quest'ultima precisazione, che ha un indubbio valore simbolico, sarebbe ingenuo ritenere che il *lifting* testuale così realizzato abbia trasformato la sostanza del modello regolatorio iscritto nella direttiva 2019/770/UE. E ciò non tanto nel senso che la differente formulazione accolta nell'art. 3, c. 1, sia del tutto priva di conseguenze operative (ad esempio in ordine all'applicabilità della disciplina dei contratti a prestazioni corrispettive). Si intende piuttosto affermare che già la formulazione originaria della Proposta di direttiva aveva un significato e una funzione diversa da quella di legittimare e far proprio un modello di pura circolazione di mercato dei dati personali. A veder le cose in maniera più distaccata, sembra che si possa affermare che l'art. 3 della proposta fosse stato concepito essenzialmente come norma di competenza, atta a stabilire il perimetro di applicabilità della direttiva e dei

[17] EDPS, *Opinion on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, n. 4/2017.

[18] EDPS, *op. ult. cit.*, p. 9; v. anche EDPS, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the digital economy*, Bruxelles, 2014, p. 8 ss.

rimedi da questa forgiati. Come si leggeva nel considerando n. 13, sotteso all'intera disciplina era l'obiettivo di realizzare un trattamento paritario di situazioni funzionalmente assimilabili sul piano della razionalità economica [19].

Escludere il modello "servizi contro dati" dall'ambito di applicazione della direttiva, e dunque negare ai consumatori i rimedi contrattuali ivi previsti, soltanto in ragione della particolare natura della controprestazione, «significherebbe discriminare alcuni modelli commerciali e incoraggerebbe in modo ingiustificato le imprese ad orientarsi verso l'offerta di contenuti digitali contro la messa a disposizione di dati. Vanno garantite condizioni di parità eque» [20].

Tale esigenza probabilmente non implicava, ma il nuovo testo fuga ogni dubbio in proposito, un *vulnus* per la normativa di protezione dei dati personali, in quanto l'art. 3, c. 8, della Proposta faceva espressamente salva l'applicabilità di tale disciplina, alla quale sarebbe spettata la definizione delle regole preordinate a stabilire i requisiti di validità e gli effetti di qualsiasi atto dispositivi di diritti sui dati personali. Un principio, quest'ultimo, ora riaffermato ed ulteriormente precisato nel nuovo art. 3, c. 8, che così stabilisce: «Il diritto dell'Unione in materia di protezione dei dati personali si applica a qualsiasi dato personale trattato in relazione ai contratti di cui al paragrafo 1. In particolare, la presente direttiva fa salvo il regolamento (UE) 2016/679 e la direttiva 2002/58/CE. In caso di conflitto tra le disposizioni della presente direttiva e del diritto dell'Unione in materia di protezione dei dati personali, prevale quest'ultimo».

Se la direttiva 2019/770/UE non fa che disciplinare alcuni aspetti dei rapporti negoziali "a valle" aventi ad oggetto la fornitura di dati personali preordinata all'accesso a servizi gratuiti, prendendo atto realisticamente del valore che assumono i dati nel contesto dell'economia 4.0, è alla normativa primaria in materia di protezione dei dati – oltre che alle regole nazionali in materia di diritto dei contratti e degli altri atti di autonomia privata – che

[19] Per un approccio di politica del diritto volto a demistificare taluni orientamenti correnti v. C. Lobet-Maris, *Du fétichisme de la donnée personelle. Relecture politique et critique de la vie privée*, in E. Degrave-C. de Terwangne-S. Dusollier (a cura di), *Law, norms and freedoms in cyberspace*, cit., pp. 685, 693 ss.

[20] Sul punto v. le riflessioni di N. Helberger-F.Z. Borgesius-A. Reyna, *The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law*, in *Common Market L. Rev.*, 54, 2017, pp. 1427 ss., 1445; G. Howells, *Reflections on Remedies for Lack of Conformity in Light of the Proposals of the EU Commission on Supply of Digital Content and Online and Other Distance Sales of Goods*, in A. De Franceschi (a cura di), *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution*, cit., p. 145 ss.

ci si deve rivolgere al fine di capire quali siano giuridicamente i limiti e le forme nelle quali l'autonomia negoziale può esprimersi in questa delicata materia. Anche su questo il considerando 38 è chiarissimo, precisando da un lato che «qualsiasi trattamento di dati personali in relazione a contratti rientranti nell'ambito di applicazione della presente direttiva è lecito solo se è conforme alle disposizioni del regolamento (UE) 2016/679»; e, dall'altro, che «[…] quando il trattamento dei dati personali si basa su un consenso, segnatamente a norma dell'articolo 6, paragrafo 1, lettera a), del regolamento (UE) 2016/679, si applicano le disposizioni specifiche di tale regolamento, comprese quelle relative alle condizioni per valutare se il consenso sia stato o meno liberamente prestato. La presente direttiva non dovrebbe disciplinare la validità del consenso prestato».

È essenziale, allora, focalizzare lo sguardo sul regolamento 2016/679/UE per capire se e a quali condizioni un atto dispositivo dei diritti sui dati personali preordinato ad ottenere l'accesso a beni o servizi offerti da un operatore economico sia valido ed efficace. Dopo aver compiuto una siffatta analisi, si dovrà ritornare al testo della direttiva 2019/770/UE per capire quale sia la disciplina di raccordo tra l'atto di consenso al trattamento dei dati e il contratto che regolamenta gli aspetti patrimoniali e negoziali della fattispecie.

3. *La disciplina del consenso nel regolamento sulla protezione dei dati personali*

La lettura del regolamento non è scevra da difficoltà. L'attenzione deve appuntarsi in particolare sull'art. 4, n. 11, che definisce il contenuto della nozione di "consenso" dell'interessato, e sull'art. 7, c. 4, che fissa con maggior precisione i requisiti sostanziali di validità di tale atto giuridico. In particolare, la prescrizione più critica è quella che attiene alla c.d. "libertà" del consenso. Il consenso, secondo l'art. 4, n. 11, è atto giuridicamente vincolante soltanto se esprime una manifestazione di volontà "libera" e informata. Quale è l'esatto significato di tale nozione? [21].

Un cultore della teoria negoziale risponderebbe immediatamente: un negozio unilaterale, come il consenso, è da reputarsi giuridicamente "libero" se non è viziato da uno dei fattori perturbativi della volontà contemplati dal quarto libro del codice civile: errore, violenza e dolo. Ma a tale assunto

[21] Per un ventaglio di ipotesi v. il saggio di T. Léonard, *Yves, si tu exploitais tes données?*, in E. Degrave-C. de Terwangne-S. Dusollier (a cura di), *Law, norms and freedoms in cyberspace*, cit., p. 659 ss., quasi interamente dedicato ai contrasti qui evidenziati.

si potrebbe agevolmente obiettare che non v'è alcuna ragione logica di ribadire espressamente in una apposita norma quanto le regole generali del negozio giuridico (o del contratto, a seconda dei modelli di riferimento) già prescrivono con cristallina chiarezza [22]. Lo stesso argomento potrebbe avanzarsi nei confronti di chi ritenga, in una prospettiva dichiaratamente anti-paternalistica, che ai fini del giudizio sulla libertà del consenso è essenziale il parametro dell'informazione: un consenso informato sarebbe di per sé un consenso libero. Tuttavia l'informazione, se è una condizione necessaria, non è invece sul piano normativo una condizione sufficiente ai fini della validità dell'atto, in quanto tale requisito è già autonomamente prescritto dal legislatore e non avrebbe senso duplicare tale concetto tramite il riferimento alla nozione di "libertà".

Per inquadrare correttamente la questione, si deve osservare che la fattispecie del consenso al trattamento dei dati è stata oggetto, a far data dall'introduzione della l. 675/1996, di una stratificata attività d'interpretazione da parte dell'autorità di regolazione (oltre che della giurisdizione ordinaria), che ha finito per attribuire alla nozione di "libertà" un contenuto più ricco ed implicante di quello ordinario [23].

In primo luogo, al requisito della libertà del consenso si è fatto ricorso al fine di negare la validità di tutte quelle manifestazioni di volontà formatesi in condizioni di pressione psicologica legata a situazioni di vulnerabilità o a strutturali asimmetrie di potere [24].

Tra gli esempi più ricorrenti, possono citarsi alcuni casi di trattamento nell'ambito dei rapporti di lavoro, quando le finalità di esso non siano strettamente necessarie all'esecuzione dell'obbligazione principale [25]. È

[22] In questo senso v. ora Cass., 2 luglio 2018, n. 17278, in *Giur. it.*, 2019, p. 530, con nota di S. Thobani, *Operazioni di* tying *e libertà del consenso* (al § 2.4).

[23] Sul punto merita di essere confrontata l'attenta analisi di S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Europa dir. priv.*, 2016, p. 513 ss.

[24] S. Ernst, *sub* § 4, in B.P. Paal-D.A. Pauly, *Datenschutz-Grundverordnung*, Beck, 2017, p. 46, Rn. 71; Art. 29 Data Protection Working Party, *Guidelines on Consent Under Regulation 2016/679*, 28 novembre 2017, 17/EN WP259, p. 7.

[25] In materia lavoristica v. ad es. garante prot. dati, provv. 28 ottobre 1999, *doc. web 47741*; nell'ambito dell'esperienza tedesca, P. Gola-C. Klug-B. Körffer-R. Schomerus, *Bundesdatenschutzgesetz Kommentar*, *sub* § 4a, München, 2015, p. 137, Rn. 22a; v. inoltre *Art. 29 Data Protection Working Party*, *Guidelines on Consent Under Regulation 2016/679*, cit., p. 8. Si noti, peraltro, che con la disciplina di adeguamento al GDPR, il legislatore tedesco ha fatto uso del margine di discrezionalità concesso dal regolamento, stabilendo requisiti di forma rafforzati in merito al consenso dell'interessato in ambito lavoristico (B. Buchner-J. Kühling, *Die Einwilligung in der Datenschutzordnung 2018*, in *DuD*, 2017, pp. 544 ss., 546).

quanto si chiarisce nel considerando 43 del regolamento, ove si legge che il consenso non può ritenersi «valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica». Non a caso, la direttiva 2016/680/UE, concernente il trattamento dei dati personali a fini di contrasto alla criminalità, investigazione di reati e attività di polizia, muove dall'assunto che il «consenso dell'interessato, quale definito nel regolamento (UE) 2016/679, non dovrebbe costituire la base giuridica per il trattamento di dati personali da parte delle autorità competenti. Qualora sia tenuto ad adempiere un obbligo legale, l'interessato non è in grado di operare una scelta autenticamente libera, pertanto la sua reazione non potrebbe essere considerata una manifestazione di volontà libera» (considerando 35).

Anche in assenza di una sostanziale disparità di potere sociale, e dunque di una sottostante pressione psicologica tale da indurre all'accettazione delle condizioni poste dal titolare del trattamento, si è ritenuto che la ponderatezza e la serenità delle scelte compiute dall'interessato possa essere inficiata dall'essere l'accesso a un bene o a un servizio – anche se non strumentale all'esercizio di una libertà fondamentale – subordinato al consenso al trattamento, qualora questo non sia strettamente necessario all'adempimento della prestazione contrattuale (c.d. *Koppelungsverbot*) [26]. Tra i molti esempi offerti dalla giurisprudenza del garante risaltano quelli della fornitura di servizi di telefonia o altri servizi online, là dove la stipula del contratto sia resa dipendente dal consenso al trattamento dei dati per finalità ulteriori, scollegate dalla causa e non necessarie all'esecuzione del contratto a monte, come quelle pubblicitarie, di *marketing* o di profilazione del cliente. Al cospetto di tali fattispecie, tutt'altro che marginali sul piano sociale e economico, l'autorità garante ha osservato che «il consenso del contraente per l'attività promozionale deve intendersi libero quando non è preimpostato e non risulta – anche solo implicitamente in via di fatto – obbligatorio per poter fruire del prodotto o servizio fornito dal titolare del trattamento. Esemplificando, non è libero il consenso prestato quando la società condiziona la registrazione al suo sito web da parte degli utenti e, conseguentemente, anche la fruizione dei suoi servizi, al rilascio del consenso al trattamento per la finalità promozionale» [27]. Non siamo lontani

[26] P. Gola-C. Klug-B. Körffer-R. Schomerus, *Bundesdatenschutzgesetz Kommentar*, *sub* § 4a, p. 136, Rn. 21.

[27] Provv. 4 luglio 2013 n. 330, doc. web n. 2542348; questa linea prosegua senza devia-

dal divieto dei *tying arrangements* iscritto nel diritto della concorrenza (cfr. art. 101, c. 1, lett. e); TFUE) [28], ma ciò che è ancor più rilevante è che la medesima posizione espressa dal garante italiano è sostanzialmente condivisa anche dalle omologhe autorità indipendenti, nonché dalla giurisprudenza nei sistemi tedesco (ove peraltro il *Koppelungsverbot* trova un'espressa formalizzazione normativa, relativamente all'uso ulteriore dei dati per finalità promozionali, nella legge federale sulla protezione dei dati personali [29]), francese e inglese [30].

Alla luce di queste premesse, e in particolare di questa comune tendenza delle autorità di regolazione nazionali, non può sorprendere che una soluzione analoga sia ora espressamente adottata dal regolamento. L'art. 7, c. 4, nel concretizzare il requisito della "libertà" del consenso posto dall'art. 4, stabilisce che «nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto».

Che tale disposizione offra un formale suggello alle soluzioni applicative sin qui emerse in diversi paesi europei è indubbio. Molto più complesso, però, è capire quali siano le implicazioni pratiche di tale norma per il tema

zioni sin dal primo significativo provvedimento del Garante nel famoso caso BNL (provv. 28 maggio 1997, doc. web 40425), ove si affermava che: «non può definirsi "libero", ma necessitato, il consenso al trattamento dei dati personali che l'interessato "deve" prestare (aderendo a un testo predisposto unilateralmente dalla controparte contrattuale) quale condizione per il conseguimento della prestazione richiesta. In tal modo, infatti, i dati personali, lecitamente raccolti dal titolare (e conferiti dall'interessato) per il perseguimento di una determinata finalità (l'esecuzione del rapporto contrattuale), vengono di fatto piegati ad un utilizzo diverso dallo scopo originario che ne aveva giustificato la raccolta, in violazione del principio di finalità».

[28] E.M. Frenzel, *sub* § 7, in B.P. Paal-D.A. Pauly, *Datenschutz-Grundverordnung*, cit., p. 115, Rn. 21.

[29] Cfr. § 28, c. 3b, BDSG: «Die verantwortliche Stelle darf den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen nach Absatz 3 Satz 1 abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Eine unter solchen Umständen erteilte Einwilligung ist unwirksam». Su questa disposizione, originariamente contenuta nel *Telemediengesetz* e poi resa di applicazione generale dopo la modifica della legge federale sulla protezione dei dati, v. G. Spindler-F. Schuster (a cura di), *Recht der Elekrtronischen Medien: Kommentar*, *sub* § 28 BDSG, München, 2015, Rn. 15-21.

[30] S. Thobani, *La libertà del consenso al trattamento dei dati personali*, cit., pp. 538-539; cui *adde* per un'analisi dell'esperienza tedesca, P. Gola-C. Klug-B. Körffer-R. Schomerus, *Bundesdatenschutzgesetz Kommentar*, *sub* § 4a, pp. 136-137, Rn. 21 ss.

che qui rileva, e in particolare per il quesito relativo all'ammissibilità di una cessione dei dati personali a titolo oneroso [31]. Si possono distinguere a tal riguardo due principali itinerari interpretativi.

Secondo il primo, il vincolo posto dall'art. 7 dovrebbe intendersi come ostativo alla validità di uno scambio tra dati personali ed altre prestazioni. Difatti, nell'escludere l'ammissibilità di un consenso preordinato a finalità ulteriori rispetto a quelle afferenti l'esecuzione della prestazione principale, ove tale consenso sia configurato dal titolare quale precondizione per l'accesso a beni e servizi, l'ordinamento esprimerebbe un netto giudizio di disvalore, tale da far ritenere che tale consenso non possa mai essere espressione di una scelta ponderata e consapevole, dunque "libera". Ora, questo è proprio quello che avviene quando servizi della società dell'informazione siano forniti gratuitamente: lo schema economico sottostante è in realtà quello dello scambio corrispettivo, ove i dati personali (da utilizzarsi tipicamente per finalità ulteriori, come la profilazione e la pubblicità mirata) costituiscono la vera controprestazione per l'accesso al servizio medesimo. Aderendo ad una lettura rigida dell'art. 7, si finirebbe necessariamente per sancire l'invalidità di un siffatto consenso (con effetti a cascata sull'intera intesa negoziale) [32].

È evidente che un risultato ermeneutico di questo tipo si rivela di fatto convergente con l'assunto per cui i dati personali non costituiscono delle "merci" e non possono essere trattati come tali. In sostanza, il modello di circolazione dei dati sarebbe sostanzialmente analogo a quello della circolazione del corpo umano, simbolicamente iscritto nell'art. 3 della Carta dei diritti fondamentali dell'Unione Europea: in entrambi i casi l'atto dispositivo dovrebbe informarsi al paradigma della gratuità, in ossequio all'idea per cui un consenso "remunerato" sarebbe per definizione un consenso "non libero" [33].

[31] Per una prima analisi del problema si segnalano in particolare i seguenti scritti: C. Langhanke-M. Schmidt-Kessel, *Consumer Data as Consideration*, cit., p. 218 ss.; A. Metzger, *Dienst Gegen Daten: Ein Synallagmatischer Vertrag*, cit., p. 816 ss.; A. Dix, *Daten als Bezahlung: Zum Verhältnis zwischen Zivilrecht und Datenschutzrecht*, in *ZEuP*, 2017, p. 1; C. Wendehorst, *Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy*, in S. Lohsse-R. Schulze-D. Staudenmayer (a cura di), *Trading Data in the Digital Economy: Legal Concepts and Tools*, cit., p. 327 ss.; M. Narciso, *'Gratuitous' Digital Content Contracts in EU Consumer Law*, cit., p. 198 ss.

[32] Pervengono sostanzialmente a questa conclusione, non senza rilievi critici nei confronti delle scelte del legislatore europeo, P. Voigt-A. von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Cham, 2017, p. 96 ss.

[33] Su questo modello v. G. Resta, voce *Doni non patrimoniali*, in *Enc. dir.*, *Annali*, IV, Giuffrè, 2011, pp. 510, p. 516 ss.

Questa tesi non riesce a persuadere, e ciò non soltanto muovendo da un'ottica giusrealistica (lo scollamento del sistema giuridico con la realtà, che conosce e legittima da lungo tempo il mercato dei dati personali, si rivelerebbe drammatico), ma già rimanendo aderenti al piano delle norme.

Vi sono almeno due argomenti, uno di natura sistematica e l'altro di natura testuale, che possono essere opposti alla prima tesi e depongono nel senso della liceità dello schema "servizi contro dati".

Il primo attiene proprio al confronto tra regime della circolazione delle parti del corpo e regime della circolazione dei dati personali. Come si è cercato di dimostrare in altra sede [34], il sistema della Carta dei diritti fondamentali dell'Unione europea, lungi dall'avvalorare l'idea della de-patrimonializzazione dei dati, la smentisce, sia pure indirettamente. Difatti, mentre con riferimento al corpo e alle sue parti si prevede espressamente che questi non possono costituire, in quanto tali, una "fonte di lucro", riprendendo letteralmente il modello francese del corpo oggetto di un diritto extra-patrimoniale (art. 16-5 *code civil*) [35], nulla di simile è stabilito con riguardo ai dati personali. L'art. 8, dopo avere ribadito la natura fondamentale del diritto alla protezione dei dati personali, menziona il consenso come una delle possibili basi idonee a giustificare il trattamento, ma non prefissa alcun limite di ordine contenutistico comparabile con quello dell'art. 3. Il che non implica che la circolazione dei dati personali debba appiattirsi sullo stesso modello della circolazione dei beni, come si avrà modo di spiegare a breve, ma certo suggerisce che l'idea della gratuità come necessario requisito di validità dell'atto non abbia ragion d'essere in relazione alla fattispecie del trattamento dei dati personali.

Il secondo argomento, si diceva, è di natura testuale e attiene alla lettera dell'art. 7 del regolamento. Qui si prevede, come si è già ricordato, che nel valutare se il consenso è stato liberamente prestato «si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto».

Escludiamo innanzitutto che l'intera questione possa essere risolta sostenendo che, poiché nello schema "servizi contro dati" il trattamento è strutturalmente necessario all'esecuzione del contratto, di esso non vi sia

[34] G. Resta, voce *Autonomia contrattuale e diritti della persona nel diritto UE*, in *Dig. disc. priv., sez. civ.*, Agg., Utet, 2013, p. 92 ss., spec. pp. 96-97; e più diffusamente Id., *La disponibilità dei diritti fondamentali e i limiti della dignità (note a margine della Carta dei diritti)*, in *Riv. dir. civ.*, 2002, II, p. 801 ss.

[35] V. ancora G. Resta, voce *Doni non patrimoniali*, cit., pp. 516-517.

necessità ai sensi dell'art. 6 del regolamento. Tale argomento sarebbe mal posto, in quanto l'art. 7 parla di libertà del consenso e ne concretizza il contenuto tramite il divieto di correlazione tra consenso e finalità ulteriori facendo riferimento alle ipotesi in cui un consenso sia necessario e dunque l'art. 6 sia inoperante [36]. D'altronde la norma parla di un trattamento "non necessario *all'esecuzione* del contratto"; mentre nello schema "servizi contro dati" il consenso è elemento strutturale dell'intesa, sì che in assenza di un trattamento lecito dei dati il contratto non verrebbe nemmeno ad esistenza, connotandosi dunque il consenso come necessario al *perfezionamento* dello stesso contratto [37].

L'argomento essenziale, ad ogni modo, consiste nel fatto che la norma non introduce un divieto, bensì stabilisce un mero parametro di valutazione, da considerare insieme ad altri (non meno rilevanti) parametri, come l'esistenza o meno di condizioni di concorrenza nel settore di riferimento, la fungibilità del bene o del servizio offerto [38] e la strumentalità rispetto all'esercizio di diritti fondamentali, la funzione di intrattenimento o professionale del servizio, l'impiego di condizioni generali di contratto senza negoziazione individuale delle clausole, ecc. [39]. Se si vuole si può anche parlare di presunzione di invalidità del consenso prestato al fine di accedere a beni o servizi, ma deve esser chiaro che si tratta di una presunzione *iuris tantum* e non, invece, *iuris et de iure.* Aderendo ad una siffatta interpretazione, vengono meno le ragioni di conflitto tra l'art. 7 del regolamento e la direttiva sulla fornitura di contenuti digitali e lo schema negoziale "servizi contro dati" può trovare una solida collocazione nel sistema [40].

Mi pare, in altri termini, che la "monetizzazione" dei dati personali non abbia in sé nulla di particolarmente disdicevole né di giuridicamente "sospetto", purché però il consenso in oggetto rappresenti una effettiva espressione dell'autodeterminazione informativa e non una fittizia clausola

[36] E.M. Frenzel, *sub* § 7, cit., p. 114, Rn. 20; T. Léonard, *Yves, si tu exploitais tes données?*, cit., pp. 677-678.

[37] E.M. Frenzel, *sub* § 7, cit., p. 114, Rn. 21.

[38] La possibilità di accedere altrove al servizio oggetto della negoziazione costituisce il principale parametro di valutazione adottato dal già citato § 28, c. 3b, BDSG; v. P. Gola-C. Klug-B. Körffer-R. Schomerus, *Bundesdatenschutzgesetz Kommentar*, *sub* § 4a, cit., p. 136, Rn. 21.

[39] Sul punto A. Metzger, *Data as Counter-Performance. What Rights and Duties do Parties Have?*, in *JIPITEC*, 8, 2017, pp. 2-5; A. Metzger, *Dienst Gegen Daten: Ein Synallagmatischer Vertrag*, cit., p. 823.

[40] In questo senso anche A. Metzger, *Dienst Gegen Daten: Ein Synallagmatischer Vertrag*, cit., p. 824.

di legittimazione dell'altrui potere negoziale o tecnologico [41]. In questo senso merita di essere specificamente richiamato un passaggio della motivazione di una recente pronunzia della Corte di cassazione che, in un caso di consenso al trattamento dei dati per finalità ultronee rispetto alla reale consistenza del servizio offerto, ha espresso in termini chiarissimi il medesimo concetto: «l'ordinamento non vieta lo scambio di dati personali, ma esige tuttavia che tale scambio sia frutto di un consenso pieno ed in nessun modo coartato» [42].

L'interrogativo da porsi, allora, è il seguente: i mercati in oggetto sono caratterizzati da un grado sufficiente di trasparenza e "libertà"? In particolare, il fornitore di dati è generalmente posto nelle condizioni di comprendere tipologie e ambiti del trattamento ulteriore dei propri dati personali, nonché l'oggettiva consistenza economica della "controprestazione non pecuniaria" coinvolta (*i.e.* i propri dati), sì da rendere possibile un reale atto di esercizio dell'autodeterminazione informativa?

A tale interrogativo non può darsi, purtroppo, una risposta sempre positiva. Il grado di opacità che caratterizza tali mercati è ancora molto elevato, e non è un caso che le autorità di regolazione della concorrenza abbiano già avuto modo di segnalare tale aspetto, condannando per violazione della normativa sulle pratiche commerciali sleali i fornitori di servizi *on line* che ottenevano l'accesso a miniere di dati personali dei consumatori carpendone il consenso attraverso lo specchietto della gratuità e condizioni generali di contratto tutt'altro che trasparenti [43].

È anche per questa ragione che si è suggerito di far discendere dagli obblighi di informazione stabiliti tanto dalla normativa sulla protezione dei dati (artt. 12-13 regolamento) quanto soprattutto da quella consumeristica (in generale v. art. 5 e ss. c. cons.), uno specifico obbligo informativo concernente la natura della controprestazione pagata dal consumatore, o persino il suo effettivo valore monetario [44]; un obbligo la cui eventuale violazione potrebbe comunque rilevare quale pratica

[41] In generale v. M. Kamp-M. Rost, *Kritik an der Einwilligung. Ein zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen*, in *DuD*, 2013, p. 80.
[42] Cass., 2 luglio 2018, n. 17278, cit. (§ 2.5).
[43] V. in particolare AGCM, 11 maggio 2017, n. 26597, *WhatsApp – Trasferimento Dati a Facebook*, in *Bollettino*, 18/2017, p. 57; Bundeskartellamt, 6 febbraio 2019, B6-22/16.
[44] Variamente, in questa prospettiva, A. De Franceschi, *Digitale Inhalte gegen Personenbezogene Daten: Unentgeltichkeit oder Gegenleistung?*, in M. Schmidt-Kessel-M. Kramme (a cura di), *Geschäftsmodelle in der digitalen Welt*, Sipplingen, 2017, pp. 113, 125-131; G. Malgieri-B. Custers, *Pricing privacy – the right to know the value of your personal data*, cit., p. 6 ss.

commerciale ingannevole ai sensi dell'art. 6 della direttiva 2005/29/CE e dell'art. 21 del codice del consumo [45]. In questa prospettiva, si è auspicato, da parte di alcuni autori, la predisposizione di opzioni di prezzo alternative (c.d. *active choice models*), comprendenti sia lo schema servizio contro dati sia quello servizio contro corrispettivo monetario [46].

Senza entrare nei dettagli di ciascuna di queste proposte interpretative, l'elemento che qui preme segnalare è che la tutela degli interessi fondamentali della persona non deve necessariamente essere perseguita attraverso un'irrealistica de-patrimonializzazione dei dati (e degli atti giuridici che ne determinano la circolazione), bensì attraverso una duplice strategia.

Da un lato si tratta di operare un attento controllo dell'atto di autonomia finalizzato ad assicurare la salvaguardia dei valori incomprimibili della personalità [47]; dall'altro, il regime prettamente privatistico di supervisione dell'atto di autonomia deve essere integrato dagli strumenti di carattere sia pubblico sia privato volti ad assicurare che il trattamento dei dati reso legittimo dalla manifestazione della volontà negoziale si conformi ad un livello elevato di rispetto delle garanzie e dei diritti della persona. Poiché questo secondo aspetto (che evoca i temi della *accountability*, del controllo da parte dell'Autorità garante, ecc.) è di specifica pertinenza delle trattazioni generali sulla normativa in materia di protezione dei dati, ci si concentrerà qui sul primo profilo indicato.

Dell'informazione si è già detto, ma non minore è il rilievo della "specificità" quale ulteriore presupposto di validità del consenso: una manifestazione di volontà generica non permette un reale apprezzamento delle concrete conseguenze dell'atto dispositivo, mentre un consenso espresso in maniera distinta e in relazione a ciascuna delle finalità rilevanti costituisce maggiore garanzia di ponderatezza delle scelte coinvolte [48]. Non è un caso che nella più recente (ed importante) pronunzia della Corte di Cassazione in materia di consenso al trattamento dei dati si sia attribuito un rilievo cruciale alla sinergia tra i due parametri di "libertà" e "specificità"

[45] N. Helberger-F.Z. Borgesius-A. Reyna, *The Perfect Match?*, cit., p. 1429.

[46] P. Hacker-B. Petkova, *Reining in the Big Promise of Big Data: Transparency, Inequality, and the New Regulatory Frontiers, Northwestern J. Techn. Int. Prop. L.*, 15, 2017, pp. 1-27.

[47] Per una più compiuta argomentazione, con riferimento all'intero spettro dei negozi sugli attributi immateriali della personalità, v. G. Resta, *Autonomia privata e diritti della personalità*, Jovene, 2005, pp. 276-284.

[48] Cfr. S. Thobani, *I requisiti del consenso al trattamento dei dati personali*, Maggioli, 2016, p. 71 ss.; e con riferimento all'intero sistema della circolazione dei diritti della personalità, G. Resta, *op. ult. cit.*, pp. 287-292.

del consenso, dichiarandosi non conforme alle prescrizione di legge un modulo di richiesta online del consenso che non dava all'interessato la possibilità di accedere al servizio senza autorizzare i trattamenti ulteriori per finalità pubblicitarie e non precisava in maniera sufficiente ambiti e limiti di tale uso secondario dei dati personali [49]. Si rivela cruciale, allora, anche in questo settore, far maturare una cultura degli operatori e specifiche prassi applicative preordinate a rafforzare la c.d. granularità del consenso.

4. *Il coordinamento tra la direttiva 2019/770 e il regolamento 2016/679*

Ciò detto quanto all'astratta compatibilità del requisito della libertà del consenso e del divieto di *tying* con la struttura economica del modello "servizi contro dati"; e ribadito che il controllo di validità del consenso deve operarsi in base ai parametri procedurali e sostanziali fissati dagli artt. 4 e 7 del regolamento, rimane da capire come si coordinino tra di loro i due plessi normativi precedentemente identificati, e segnatamente il regolamento 2016/679/UE e la direttiva 2019/770/UE. Senza che sia qui necessario soffermarsi sulle questioni minutamente esegetiche e di dettaglio, converrà concentrare l'attenzione su un problema di fondo: quale è il rapporto tra il consenso al trattamento dei dati disciplinato dal regolamento e il contratto di fornitura di servizi e contenuti digitali disciplinato (dal diritto nazionale

[49] Cfr. Cass., 2 luglio 2018, n. 17278, cit., al § 2.6, ove si legge che: «oltre che libero, il consenso […] deve essere specifico: ed è manifesto che il requisito della specificità si pone, nel disegno normativo, in stretto collegamento con quello della libertà del consenso, così da risolversi in un'endiadi, giacché la libertà della determinazione volitiva in ordine al trattamento dei dati personali non sarebbe neppure astrattamente configurabile, nel suo atteggiarsi quale consenso informato, se non fosse univocamente indirizzata alla produzione di effetti che l'utente abbia preventivamente avuto modo di rappresentarsi, singolarmente, con esattezza. L'interessato deve essere allora con certezza posto nella condizione di raffigurarsi, in maniera inequivocabile, gli effetti del consenso prestato al trattamento dei suoi dati: di guisa che, se detto consenso comporta una pluralità di effetti – come nel caso di specie, in cui esso si estende alla ricezione di messaggi promozionali anche da parte di terzi –, lo stesso va singolarmente prestato in riferimento a ciascuno di essi, di modo che, con totale trasparenza, risulti palese che proprio ciascuno di tali effetti egli ha voluto. È dunque senz'altro da escludere che il consenso possa dirsi specificamente, e dunque anche liberamente prestato, in un'ipotesi in cui, ove gli effetti del consenso non siano indicati con completezza accanto ad una specifica "spunta" apposta sulla relativa cartella di una pagina Web, ma siano invece descritti in altra pagina Web linkata alla prima, non vi sia contezza che l'interessato abbia consultato detta altra pagina, apponendo nuovamente una diversa "spunta" finalizzata a manifestare il suo consenso».

dei contratti, come determinato dal regolamento 593/2008/UE sul diritto applicabile alle obbligazioni contrattuali, e) dalla direttiva?

Ragioni testuali e logiche inducono a ritenere che, benché si tratti di un'operazione economicamente unitaria, giuridicamente il consenso al trattamento e il contratto di accesso al servizio rappresentano due atti distinti e sottoposti ciascuno a una specifica disciplina [50].

Il consenso costituisce un atto a struttura unilaterale (sia pure perfezionato, di norma, a seguito di specifica sollecitazione della controparte), il quale funzionalmente realizza l'esercizio del diritto di "autodeterminazione informativa" [51]. Discutere se esso configuri un atto negoziale o non negoziale porta a poco, perché anche a ritenere – cosa che sembra più lineare – che si tratti di un vero e proprio negozio giuridico, le regole applicabili alla fattispecie – ad es. in punto di capacità, vizi del volere, etc. – dovranno essere comunque teleologicamente adattate alla peculiare natura degli interessi coinvolti. La disciplina forgiata dal legislatore comunitario indica chiaramente che il consenso non può essere parificato ad un qualsiasi altro atto negoziale. Come si è già visto nel paragrafo precedente, i requisiti della "libertà", dell'"informazione" e della "specificità" fissano uno standard di validità – nel senso di idoneità a produrre l'effetto legittimante di cui all'art. 6 del regolamento – che è molto più elevato rispetto a quello consueto per gli atti patrimoniali ed è volto a garantire che l'atto veicoli una reale determinazione volitiva del soggetto. Valorizzando uno spunto presente nella sentenza della Corte di cassazione precedentemente ricordata, il consenso al trattamento dei dati è giuridicamente più prossimo al consenso informato al trattamento medico che non al prototipo degli atti negoziali a contenuto patrimoniale. Come tale, il giudizio sulla sua validità/efficacia scriminante deve essere condotto alla luce delle norme specificamente previste nel regolamento e deve tenere adeguatamente conto della peculiare funzione di tale atto in quanto strumento d'esercizio dell'autodeterminazione informativa.

Il contratto di fornitura di servizi e contenuti digitali, per contro, opera logicamente "a valle" rispetto al consenso, il quale costituisce il presupposto indispensabile, l'elemento legittimante "a monte", perché possa aversi un lecito trattamento dei dati personali (sempre che, s'intende, non sussista altra base giuridica di riferimento ai sensi dell'art. 6 del regolamento). A questo riguardo è bene insistere sul carattere logicamente obbligato della sequenza

[50] In questo senso si è espresso, di recente, anche G. De Cristofaro, *Die Datenschutzrechtliche Einwilligung als Gegenstand des Leistungsversprechens*, v. *infra*, nota 53.

[51] In quest'ottica, da ultimo, B. Buchner-J. Kühling, *Die Einwilligung in der Datenschutzordnung 2018*, cit., spec. p. 545.

descritta, quand'anche nella prassi i due momenti siano temporalmente unitari o indistinguibili sul piano del *drafting* contrattuale (è noto infatti che il "consenso" al trattamento è sovente reso attraverso clausole integrate in modelli standard). Prima viene il consenso che "abilita" la negoziazione bilaterale, conformando modalità e limiti del trattamento; poi viene il contratto, che regola gli aspetti essenzialmente patrimoniali e definisce il programma obbligatorio del rapporto, prevedendo ad esempio l'accesso a servizi o contenuti digitali in cambio della fornitura di (o dell'impegno a fornire) dati personali [52].

Non potrebbe darsi, invece, una scansione logica opposta, in quanto non sarebbe giuridicamente configurabile un contratto che produca l'obbligo per l'interessato di prestare il consenso al trattamento dei dati personali. Un siffatto consenso, reso in esecuzione di uno specifico obbligo di fonte contrattuale, sarebbe infatti ontologicamente incompatibile con il prototipo normativo del "consenso libero" [53]; il contratto, per suo conto, rischierebbe di risultare viziato per conflitto con norme imperative, le quali prescrivono appunto l'incoercibilità del consenso al trattamento.

La distinzione in oggetto – la quale, si ribadisce, va riferita al piano logico dell'analisi e non necessariamente a quello fenomenologico – è giuridicamente rilevante da un duplice punto di vista.

Innanzitutto ne discende l'esigenza di un trattamento differenziato dei due atti giuridici coinvolti: come si è chiarito in precedenza, il consenso è soggetto alla disciplina del regolamento, ha una sua specificità ed è connotata dagli elementi precedentemente illustrati, mentre il contratto è soggetto alle diverse regole derivanti dal diritto interno e dalle fonti europee, siano queste le regole generali o quelle preordinate alla tutela dei consumatori.

Ciò implica, ad esempio, che i requisiti di capacità prescritti per il valido compimento dell'atto sono diversi per il consenso e per il contratto: i primi posti dall'art. 8 del regolamento, come declinato nel nostro ordinamento dall'art. 2-*quinquies*, c. 1 del codice in materia di protezione dei dati (quattordici anni d'età); i secondi dalla norma generale dell'art.

[52] Secondo la nota prospettazione di D. Messinetti, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, pp. 339, 365; sul punto v. ora T. Léonard, *Yves, si tu exploitais tes données?*, cit., pp. 666-668.

[53] In quest'ottica v. G. De Cristofaro, *Die Datenschutzrechtliche Einwilligung als Gegenstand des Leistungsversprechens* e T. Riehm, *Freie Widerruflichkeit der Einwilligung und Struktur der Obligation*, relazioni presentate al Convegno "Rechte an Daten", Università di Bayreuth, 21-22 febbraio 2019, i cui atti sono di prossima pubblicazione.

2 del codice civile (maggiore età) [54]. Sicché il consenso al trattamento dei dati potrebbe essere validamente rilasciato dal minore ultraquattordicenne, mentre il contratto di accesso al servizio di social network richiede l'assenso degli esercenti la potestà genitoriale [55].

Del pari, dovrebbe logicamente ritenersi che la normativa sulle clausole vessatorie (artt. 33 e ss. c. cons.; direttiva 93/13/CE) non sia di per sé direttamente applicabile al consenso in quanto atto unilaterale di esercizio del diritto di autodeterminazione informativa. Essa rappresenta, però, un ineludibile punto di riferimento per l'ipotesi in cui il consenso sia integrato all'interno di moduli e formulari. E ciò non soltanto nel senso che le clausole di richiesta del consenso o le *privacy policies* accessorie ad un più ampio accordo contrattuale possono essere oggetto di specifico scrutinio ai sensi della normativa consumeristica, come testimoniato da un importante indirizzo emerso nella giurisprudenza tedesca [56]; ma anche che il giudizio sulla libertà e consapevolezza del consenso, come ribadito dal considerando 42 del regolamento, non potrà non tener conto dei criteri direttivi prefissati dalla disciplina consumeristica. In particolare, si dovrà tenere presente quanto previsto dal secondo comma dell'art. 8 del regolamento, ai sensi del quale se il consenso «è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro». Si tratta del fondamentale paradigma del *Trennungsprinzip*, il quale traduce in specifico canone operativo il principio di trasparenza relativamente alla manifestazione di consenso: la dichiarazione di consenso, per essere tale, deve appuntarsi su uno specifico progetto di trattamento, rappresentato in maniera univoca e distinguibile dalle altre materie su cui insiste l'accordo negoziale. È da chiarire, a tal riguardo, che l'eventuale violazione di tale principio ha per conseguenza la mera invalidità dell'atto di consenso ai sensi dell'art. 7 del regolamento, la quale non travolge automaticamente l'intera intesa contrattuale, la quale rimane soggetta agli specifici meccanismi di controllo e di sindacato dettati dal diritto comune e dal diritto dei consumatori [57].

Particolarmente rilevante, a tal proposito, può rilevarsi il ricorso

[54] Cfr. art. 8, c. 3, regolamento 2016/679/UE.

[55] Sul punto A. Metzger, *Data as Counter-Performance*, cit., p. 4.

[56] Sul punto e per riferimenti, N. Helberger-F.Z. Borgesius-A. Reyna, *The Perfect Match?*, cit., p. 1452.

[57] P. Schmechel, *Verbraucherdatenschutzrecht in der EU-Datenschutzgrundverordnung*, cit., pp. 280-281.

alla disciplina delle pratiche commerciali scorrette ai sensi della direttiva 2005/29/CE, in quanto in tal caso la valutazione si appunta necessariamente sull'intera operazione negoziale, al fine di sanzionare quei comportamenti dell'operatore economico atti a condizionare la libertà di scelta e a orientare le decisioni di natura commerciale dei consumatori [58]. Alcune importanti decisioni di corti e autorità indipendenti hanno fatto rientrare tra i comportamenti incriminati le pratiche commerciali volte ad ottenere il consenso al trattamento dei dati personali in maniera ingannevole o aggressiva, impedendo un effettivo esercizio della libertà di autodeterminazione [59]. Il caso più noto, a questo riguardo, è quello dell'acquisizione di Whatsapp da parte di Facebook, pesantemente sanzionato da parte dell'Autorità garante per la concorrenza e il mercato [60].

In secondo luogo, dall'assenza di una struttura negoziale unitaria discende l'impossibilità logica di configurare l'atto giuridico di consenso, in quanto tale, elemento costitutivo del sinallagma contrattuale [61]. Essa non esclude, però, che tra il consenso unilaterale al trattamento e il contratto di fornitura di contenuti e servizi digitali intercorra uno specifico collegamento.

Ciò ha un significato particolare per il caso di vizi genetici o sopravvenuti del rapporto. Dalla sussistenza di un collegamento negoziale discende, in particolare, che l'eventuale declaratoria di invalidità del consenso per contrasto con i requisiti prescritti dall'art. 7 del regolamento, benché non determini automaticamente l'inefficacia del contratto, possa astrattamente legittimare lo scioglimento del vincolo qualora si dimostri che la possibilità di procedere ad un lecito trattamento dei dati personali costituisse, nell'economia del rapporto, una vera e propria "base negoziale".

[58] In tema N. Helberger-F.Z. Borgesius-A. Reyna, *The Perfect Match?*, cit., p. 1454; per un inquadramento più generale v. G. Guizzi, *Il divieto delle pratiche commerciali scorrette tra tutela del consumatore, tutela del concorrente e tutela del mercato: nuove prospettive (con qualche inquietudine) nella disciplina della concorrenza sleale*, in A. Gambino (a cura di), *Rimedi e tecniche di protezione del consumatore*, Giappichelli, 2011, 297 ss.

[59] Per riferimenti N. Helberger-F.Z. Borgesius-A. Reyna, *The Perfect Match?*, cit., p. 1454.

[60] V. in particolare AGCM, 11 maggio 2017, n. 26597, *WhatsApp – Trasferimento Dati a Facebook*, in *Bollettino*, n. 18/2017, p. 57; v. altresì Bundeskartellamt, 6 febbraio 2019, B6-22/16, in *BeckRS*, 2019, 4895; BGH, 14 gennaio 2016, in *GRUR*, 2016, p. 946, concernente la funzione "trova amici" di Facebook e il rilievo consumeristico della disciplina in materia di protezione dei dati.

[61] Così T. Riehm, *Freie Widerruflichkeit der Einwilligung und Struktur der Obligation*, cit.; diversamente A. Metzger, *Data as Counter-Performance*, cit., p. 6, ma in costanza della versione originaria della proposta di direttiva.

Soprattutto, il nesso funzionale tra i due atti giuridici fa sì che, in caso di revoca del consenso, anche il vincolo contrattuale sia destinato a venir meno, in quanto dalla revoca deriva la caducazione con effetto *ex nunc* della base primaria di legittimazione al trattamento dei dati. Di riflesso, l'equilibrio originario tra le prestazioni (servizi contro dati) ne viene inesorabilmente sconvolto, con conseguente legittimazione dell'altro contraente a invocare la liberazione dagli obblighi primari di prestazione assunti con la stipula del contratto di fornitura di servizi e contenuti digitali.

Dogmaticamente, la fattispecie si presta a diverse alternative ricostruttive. Si potrebbe, ad esempio, ravvisare un contratto risolutivamente condizionato alla persistenza del consenso al trattamento dei dati (ma ci si esporrebbe all'obiezione per cui la condizione in oggetto avrebbe carattere "meramente potestativo"); un contratto soggetto al rimedio risolutorio *ex* art. 1467 c.c. (o in base alla regola generale di buona fede) per il venir meno della "presupposizione" cui le parti avevano subordinato l'adesione all'intesa negoziale [62]; un recesso unilaterale dal contratto di durata [63].

Approfondire ciascuna di queste opzioni analitiche sarebbe indubbiamente affascinante sul piano teorico [64], ma non è indispensabile su quello operazionale. Quale che sia la ricostruzione che si prediliga, un punto deve essere, infatti, tenuto fermo, e cioè che la caducazione del vincolo contrattuale non può determinare conseguenze pregiudizievoli in capo al revocante. In altri termini, la revoca del consenso – e così pure l'esercizio degli altri diritti dell'interessato suscettibili di interferire con l'esecuzione del contratto – non può produrre alcun obbligo di risarcimento o indennizzo per la frustrazione delle aspettative riposte dalla controparte nella stabilità del rapporto contrattuale, poiché se così fosse il consenso non potrebbe ritenersi conforme al paradigma normativo – l'art.

[62] Circa la dottrina delle sopravvenienze e la rilevanza normativa della c.d. presupposizione v. in luogo di molti F. Macario, *Le sopravvenienze*, in *Tratt. Roppo*, V, *Rimedi – 2*, Giuffrè, 2006, p. 517 ss. Non credo invece possa invocarsi l'istituto della risoluzione per impossibilità sopravvenuta, in quanto la disponibilità dei dati non sempre costituisce elemento indispensabile per l'erogazione del servizio e per l'attuazione del programma negoziale, come dimostra il caso delle piattaforme "a più versanti", nelle quali è la semplice disponibilità di un'unità aggiuntiva di utenti del servizio (anche a prescindere dunque dall'accesso ai relativi dati) a dar valore all'apporto della controparte e dunque a giustificare la continuazione dell'erogazione del servizio a titolo gratuito.

[63] Su disciplina e tipologie dei recessi unilaterali v. P. Sirena, *Effetti e vincolo*, in *Tratt. Roppo*, III, *Effetti*, Giuffrè, 2006, p. 113 ss.

[64] Alcune delle principali alternative dogmatiche sono state tratteggiate e discusse, con riferimento al diritto tedesco, nella già citata relazione di T. Riehm, *Freie Widerruflichkeit der Einwilligung und Struktur der Obligation*, cit.

7, c. 3 del regolamento prescrive che «il consenso è revocato con la stessa facilità con cui è accordato» [65] – e pertanto l'intero trattamento dovrebbe reputarsi condotto in violazione di legge [66].

Del pari, l'eventuale inadempimento da parte dell'operatore economico dell'obbligo di fornire servizi e contenuti digitali, come pure la fornitura di servizi e contenuti non conformi ai sensi degli artt. 7, 8 e 9 della direttiva 2019/770/UE, non legittima soltanto l'esercizio da parte del consumatore del diritto di recesso o di risoluzione del contratto alla stregua degli artt. 13 e 14, ma a maggior ragione può rafforzare costui nell'intento di revocare il consenso al trattamento. Anzi, è da ritenere che una revoca sia presuntivamente inclusa nella dichiarazione di recesso dal contratto. Ad ogni modo, lo stesso principio di finalità potrebbe essere d'ostacolo alla prosecuzione di un trattamento funzionalmente preordinato all'esecuzione di un rapporto contrattuale successivamente esauritosi, determinando dunque l'obbligo di cancellazione o trasformazione in forma anonima dei dati. In questo senso è opportuno il chiarimento espresso nell'art. 16, c. 2, della direttiva 2019/ 770/UE, ove si prevede che, in caso di risoluzione, «[p]er quanto riguarda i dati personali del consumatore, l'operatore economico rispetta gli obblighi applicabili a norma del regolamento (UE) 2016/679».

5. *Conclusioni*

Le ultime considerazioni svolte fanno riemergere un profilo già toccato in precedenza e che merita qui di essere ripreso a mo' di conclusione del discorso.

L'assunto della non equiparabilità dei dati ad una merce, iscritto nel considerando 24 della direttiva 2019/770, non implica necessariamente l'impossibilità di addivenire a schemi di remunerazione del consenso, com'è tipico, appunto, dei modelli servizi contro dati. Non diversamente da quanto sostenuto in ordine alla circolazione degli attributi della personalità suscettibili di sfruttamento commerciale, il legame con la persona impone invece l'applicazione di un sistema di regole – le quali vanno dalla tutela dei

[65] In tema v. E.M. Frenzel, *sub* § 7, cit., p. 113, Rn. 16-17; per una ricognizione dei termini in cui si era sviluppato il dibattito italiano sulla revocabilità v. G. Resta, *Revoca del consenso e interesse al trattamento nella legge sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 2000, p. 299 ss.

[66] Cfr. il considerando 42 del regolamento.

diritti dell'interessato di cui agli artt. 15-20 del regolamento [67] al principio della strutturale precarietà dei rapporti inerenti il trattamento dei dati *ex* art. 7 – che conformi il rapporto in maniera garantistica e rispettosa dei precetti di tutela della dignità umana e degli altri diritti fondamentali. La de-patrimonializzazione non è, in altri termini, una strategia che il diritto può realisticamente perseguire, confidando di invertire processi sociali, economici e tecnologici ormai fortemente radicati a livello globale. Ciò che invece l'ordinamento può e deve realizzare è un'infrastruttura normativa idonea a incanalare l'esercizio dell'autonomia privata all'interno di un quadro di regole condivise e trasparenti, connotate, com'è nello spirito del diritto europeo, dalla prevalenza dei diritti sulle logiche di autoregolazione del mercato.

L'interferenza tra il diritto alla protezione dei dati e il sistema dei contratti su contenuti digitali è, da questo punto di vista, un caso di studio esemplare, non meno di quanto lo sia stato, in passato, l'interazione tra prerogative morali dell'autore e contratto di edizione, o di quanto lo sia, ancor oggi, il rapporto tra diritti della personalità e *merchandising*.

La principale differenza sta nella maggiore capillarità e diffusione del fenomeno della "patrimonializzazione" dei dati, che non tocca più soltanto la cerchia ristretta degli autori o delle persone note, ma tutti noi in quanto consumatori, utenti della rete e in genere individui costantemente immersi in flussi di informazioni in entrata e in uscita.

Anche per questa ragione è importante ricordare che il controllo sull'autonomia privata non deve essere inteso in una prospettiva meramente privatistica, ma, come ha insegnato Stefano Rodotà, è un elemento integrale del controllo democratico sul potere, e in particolare sul potere derivante dalle informazioni [68]. Esso è parte, necessariamente, di quella "strategia giuridica integrata", che, nel combinare strumenti privatistici e pubblicistici, tecniche procedurali e sostanziali, controlli individuali e controlli collettivi, intende dare un contenuto sostanziale all'idea della protezione dei dati come diritto fondamentale, la quale – come ci ricorda l'art. 8 della Carta dei diritti fondamentali UE – è un elemento connotativo dell'identità costituzionale europea. È opportuno, da questo punto di vista, richiamare

[67] Sui suddetti diritti dell'interessato v. P. Voigt-A. von dem Bussche, *The EU General Data Protection Regulation (GDPR)*, cit., p. 141 ss.; A. Ricci, in G. Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla* privacy *e sulla protezione dei dati personali*, Zanichelli, 2017, p. 179 ss.

[68] V. già. S. Rodotà, *Elaboratori elettronici e controllo sociale*, Il Mulino, 1973 (ristampa inalterata, Jovene 2018); Id., *Protezione dei dati e circolazione delle informazioni*, in *Tecnologie e diritti*, Il Mulino, 1995, p. 93.

l'attenzione sull'art. 21 della direttiva 2019/770/UE, che demanda agli Stati Membri la predisposizione di strumenti adeguati al fine di garantire l'osservanza della direttiva, e tra questi sono espressamente contemplate le disposizioni del diritto interno volte a permettere l'esercizio in forma collettiva – da parte di "organizzazioni di consumatori aventi un interesse legittimo a proteggere i consumatori" oppure da "organismi, organizzazioni o associazioni senza scopo di lucro, attivi nel settore della protezione dei diritti e delle libertà degli interessati di cui all'art. 80 del regolamento (UE) 2016/679 – dei rimedi spettanti al cittadino-consumatore. Si tratta di un'ulteriore testimonianza della crescente convergenza del diritto dei consumatori e del diritto della protezione dei dati nel contesto della società digitale; una convergenza resa necessaria dall'evoluzione dei rapporti economici, che rendono i dati degli utenti sempre più un elemento centrale dei rapporti di produzione e consumo [69].

[69] Sul punto N. Helberger-F.Z. Borgesius-A. Reyna, *The Perfect Match?*, cit., p. 1427; P. Schmechel, *Verbraucherdatenschutzrecht in der EU-Datenschutzgrundverordnung*, in H. Micklitz-L.A. Reisch *et al.* (a cura di), *Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt*, Baden-Baden, 2017, p. 265 ss.

Andrea Vigorito

Postmortem Exercise of Data Protection Rights: The Apple Case

Abstract. The paper aims at developing the debate on digital inheritance by analyzing its first judicial application in Italy. In this decision, the Court applied Article 2-terdecies, d.lgs 196/2003 and took a crucial step with regard to the legal regime of personal data – and, more broadly, of digital resources – after the data subject's death. The Italian legislation, as this decision shows, seems to have adopted a 'personalistic model' through which not only heirs and relatives, but any person showing a legitimate interest could exercise the data subject's rights on personal data. After a brief introduction of the main themes concerning the postmortal exercise of data (1.), this essay analyzes the reasons behind the judicial decision (2.) and seeks to further explore the dogmatic qualification of the rights on personal data recognized by the legislator with Article 2-terdecies (3.).

1. *Data perpetuity in the information society*

'*We live on the internet, but what happens when we die there?*'[1] The debate surrounding the correct framing of the legal regime of digital resources is currently involving the time span following the death of an individual. The topic has been gaining momentum in the scholarly studies and it has recently found a concrete example in our legal system with the first judicial case decided by an Italian court concerning postmortem access to personal data, decided by the first civil section of the Court of Milan.

The extension of the scope of application of the debate inherent to the digital goods' legal regime to the post-mortal phase arises as a logical corollary of the 'commodification' process that affects the goods of the information society. Indeed, a variety of socioeconomic rationales are traditionally identified for the relevance recognized to the issue of 'digital death'[2] and are deeply connected with the centrality that digital resources

* This article was first published in the *Roma Tre Law Review*, 2, 2021, pp. 83-92.

[1] N.M. Banta, *Inherit the Cloud: The Role of Private Contracts in Distributing or Deleting Digital Assets at Death*, in *Fordham L. Rev.*, vol. 83, 2014, p. 799, at 800.

[2] G. Resta, *La "morte" digitale*, in *Dir. inf.*, 6, 2014, pp. 891-920.

such as data have reached within the digital economy[3]. Within this framework, many economic actors are flourishing and developing the so-called 'Digital Afterlife Industry' (DAI)[4]: the trend of stratification and exploitation of data belonging to deceased individuals finds its origin in empirical evidence such as, on the one hand, the (over)accumulation[5] of profiles (and, therefore, information) of deceased persons on social networks and, on the other hand, the spreading of for-profit enterprises that focus their commercial practices on data.

This depicted tendency has provoked, in many areas, a rethinking[6] of the relationship between the single individual and the end of life[7] in light of the new information society's paradigms. Consequently, numerous questions of legal nature are arising as well; amongst them, particular attention has been addressed to the so-called 'digital inheritance.'

For obvious reasons, the studies inherent to data 'perpetuity'[8] have mostly focused on governing data related to living individuals, in line with the enhancement of forms of protection such as the right to be forgotten[9]. Since few years, however, the attention of scholars has turned to the theorization

[3] Summarized by ID., *Personal Data and Digital Assets after Death: a Comparative Law Perspective on the BGH* Facebook *Ruling*, in *EuCML*, 5, 2018, p. 201, at 201-202.

[4] C.J. Öhman, L. Floridi, *The Political Economy of Death in the Age of Information: A Critical Approach to the Digital Afterlife Industry*, *Minds and Machines*, 27, 2017, pp. 639-662. Specifically, regarding the policy choices made by Facebook, see D. Mccallig, *Facebook after death: an evolving policy in a social network*, in *International Journal of Law and Information Technology*, 22/2, 2014, pp. 107-140.

[5] It has been calculated that, if Facebook continues to attract new users and expand with the same rate, the number of deceased users will exceed 4.9 billion before 2100. The statistic is reported by C.J. Öhman, D. Watson, *Are the dead taking over Facebook? A Big Data approach to the future of death online*, in *Big Data & Society*, *January-June* 2019, pp. 1-13.

[6] T. Walter, *The pervasive dead*, in *Mortality*, 24/4, 2019, pp. 389-404 points out that a 'pervasivity' model of death is spreading and that it is characterized by the continuation of bonds even after the event of dying, moving away from the paradigm of death as a place without return (that dates back to Catullus, 3, 11-12: "*Qui nunc it per iter tenebricosum/illuc, unde negant redire quemquam*").

[7] D. Sisto, *Morte e immortalità digitale: la vita dei dati online e l'interazione postuma*, in *Funes. Journal of narratives and social sciences*, vol. 2, 2018, p. 111, at 111.

[8] Resta, *La "morte" digitale*, cit., at p. 892.

[9] Among the many scholars who have been dealing with the topic, see G. Finocchiaro, *Il diritto all'oblio nel Quadro dei diritti della personalità*, in *Dir. inf.*, 4-5, 2014, pp. 591-604; M.R. Morelli, *Oblio (diritto all')*, in *Enc. dir.*, Agg. VI, Milano, 2002; J. Rosen, *The Right To Be Forgotten*, in *Stan. L. Rev. Online* 64, 2012, pp. 88-92; also, naturally, on a case-law basis, see ECJ 13 May 2014, C-131/12, *Google Spain SL, Google Inc. contro Agencia Española de protecciòn de datos (AEPD) e Mario Costeja Gonzàles*.

and identification of forms of protection aimed at pursuing an adequate data access model or governance model also related to deceased people[10].

At least in part, the shift is due to the fact that the same problem of the 'dissociation'[11] between digital identity and personal identity affects the individual both in life and after death[12]. In fact, it could be argued that this dissociation reaches it's acme at the moment of the separation between the digital identity of the deceased and his physical body: for the living individual, the dissociation affects his identity, which is disjointed into a plurality of digital identities, distinct from each other by place of storage and respective temporal frame of reference; instead, with regard to the deceased, the disappearance of the physical body is not balanced by the disappearance of the 'electronic'[13] one, which, indeed, outlives it.

The fact that the physical body is survived by the digital alter ego should not be overlooked, since the latter keeps existing in countless formats and for an incalculable time[14]. As a consequence, the expression digital 'immortality' is becoming increasingly popular among scholars[15].

Therefore, the outlined scenario justifies the efforts to clarify the fate of digital assets relating to an individual after his/her death. Correspondingly, judges have to deal with challenges arising on two levels: firstly, the identification and legal qualification of tools and remedies that can be implemented with the purpose of providing effective post-mortal protection of the rights; secondly, judicial decisions should address the internet as a whole, in order to prevent the protection's nullification due to the inherent 'aterritorial' nature of data[16].

[10] In the Italian context, see M. Cinque, *La successione nel "patrimonio digitale": prime considerazioni*, in *Nuova giur. civ. comm.*, 2012, II; A. Magnani, *L'eredità digitale*, *Notariato*, 2014, pp. 519-532; V. Barba, *Interessi* post mortem *tra testamento e altri atti di ultima volontà*, in *Riv. dir. civ.*, 2017, pp. 319-349; C. Camardi, *L'eredità digitale. Tra reale e virtuale*, in *Dir. inf.*, 1, 2018, pp. 65-93.

[11] Resta, *La "morte" digitale*, cit., at p. 892, where the Author specifies that this dissociation disjoints in a synchronic dimension (data accumulated in a plurality of archives) and in a diachronic one (the reputation of the person remains inherently dependent on the events of the past).

[12] Resta, *Identità personale e identità digitale*, in *Dir. inf.*, 3, 2007, pp. 511-531.

[13] S. Rodotà, *Il diritto di avere diritti*, Roma-Bari, Editori Laterza, 2012, p. 397.

[14] Sisto, *Digital Death. Le trasformazioni digitali della morte e del lutto*, *Lessico di etica pubblica*, 1, 2018, p. 49, at 57.

[15] Sisto, *Morte e immortalità digitale…*, cit., pp. 111-122.

[16] J. Daskal, *The Un-Territoriality od Data*, *The Yale Law Journal*, 125, 2015, pp. 326-398. In this context, data is understood as part of the 'digital heritage' to which the digital inheritance pertains (for this expression, see Cinque, *La successione nel "patrimonio digitale"…*, cit., pp. 645-655).

A first step in addressing these issues was taken by the decision of Court of Milan pertaining to the subject of this essay.

2. *The ruling*

In accordance with Articles 669-*bis* and 700 c.p.c., the parents of a man deceased in a car accident appealed to the Court of Milan to obtain assistance from Apple in the recovery of their son's personal data. Data created with the physical device – destroyed in the accident – was stored in the iCloud account thanks to the synchronization system, but the parents, despite their requests, were not allowed to access it, due to the restrictions Apple applied.

Once established the admissibility of the legal request, the reasoning of the Court departs from the innovative legal provision introduced by D.lgs. 10 agosto 2018, n. 101, i.e. Article 2-*terdecies* of the Italian Data Protection Code (D.lgs. 30 giugno 2003, n. 196).

The ground-breaking rule, that follows the guidance of the GDPR[17] and whose function is explicitly to ensure regulatory coverage to postmortal data protection, states that the rights provided by Arts. 15 to 22 of the GDPR can be exercised by the ones who have an interest, or act in the protection of the deceased, or due to family reasons.

In the specific case, the Court deals with the request of recognizing the right of access under Article 15 GDPR.

On the basis of Article 2-*terdecies*, by referring to the 'family reasons worthy of protection' identified in the provision, the Court stated that the plaintiffs were entitled to exercise the right to access to the deceased son's personal data. The judge has pointed out, indeed, that the bond existing between parents and children, the content of the allegations and the desire of collecting a selection of recipes which their son – working as a chef – had saved in the device, were conditions that could justify the provision's

[17] Recital n. 27 specifies that the Regulation does not apply to this kind of data ('This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons'), due to a choice that has been defined coherent with the traditional principle that legislative policy decisions regarding family law or succession law exceed the legislative competence of the European Union (F. Trolli, *La successione* mortis causa *nei dati personali del defunto e i limiti al loro trattamento*, in *Jus Civile*, 4, 2019, p. 313, at 318).

application[18].

Given the admissibility of the appeal and the legitimacy to access the data of the deceased, the Court's logical reasoning unfolds by taking into consideration the possible reasons that could have precluded the approval of the requested measure: on the one hand, the limits that the legislative framework places on the postmortem exercise of the rights on personal data and, on the other hand, the conditions that the procedural discipline requires for the preventive measure under Article 700 c.p.c.

With regard to the first set of limits, Article 2-*terdecies*, II, Data Protection Code enhances the autonomy of the data subject and allows him/her to 'prohibit' the exercise of the rights on personal data after the event of death. However, neither an explicit will nor its specific formal and substantive requirements can be found in the present case.

Therefore, the judge could admit the legitimacy of the plaintiffs.

With regard to the second set of limits, the Court considered both the *fumus boni iuris* and the *periculum in mora* as existing. The first was recognized because of the legitimacy to exercise the right to access personal data[19]. The second was claimed as actual due to the fact that the Apple systems related to the deceased person would have been definitively 'destroyed' following a period of inactivity of the user, with the consequence of the loss of the data stored and, hence, the irreparable damage to the exercise of the recognized rights.

For the reasons briefly summarized here, the Court sentenced Apple 'to provide assistance […] in the recovery of data from the accounts […] in the procedure called «transfer», aimed at allowing the applicants to acquire the credentials of access to Apple ID'[20].

3. *Postmortem exercise of data protection rights*

The decision of the Court of Milan addresses, for the first time in our legal system, at a case law level, the issue of 'digital inheritance.' This expression identifies the problem inherent to the fate of data and, more generally, of digital goods, after the death of an individual.

[18] Trib. Milano, ord. 10.02.2021, p. 5.

[19] The judge follows this hermeneutic path by coordinating the national discipline with the principles expressed by the GDPR. In particular, the reasoning is shown by the reference to the 'legitimate interest' mentioned by Article 6, par. 1, lett. f) GDPR, that makes the processing of data 'lawful'.

[20] Trib. Milano, ord. 10.02.2021, p. 7.

The *quaestio iuris* lies on the thin line along succession law and personality rights and it is emphasized by a phenomenological element: the dissociation between an individual's biological existence and his/her electronic double[21]. In addition to this aspect, another, more recent phenomenological factor arises, the concrete implications of which are yet to be determined: the consequences of the aterritorial nature of data in terms of circulation of digital goods. The aterritoriality raises questions concerning the individuation and coordination of regulatory measures which should be implemented with respect to data. Indeed, it may occur that the effectiveness of legal protection could be frustrated due to the continuous crossing of territorial borders and, consequently, of jurisdictions, by data and by digital goods in general.

The mentioned decision offers some particularly interesting insights.

In order to define the rights on personal data of a deceased user, it is necessary to preliminarily address the concrete structure that the 'digital heritage' can assume. A patrimonial component should be distinguished from an affective one[22]. Moreover, the interest may be directed both to data access and to their governance[23].

The interesting aspect emerging from the ruling of the Court of Milan concerns the practical application of the new Article 2-*terdecies*, D.lgs. 196/2003, introduced by D.lgs. 101/2018, through which the Italian legislator confirms the theoretical approach of the previous legal framework[24]. This approach, according to some scholars, aligned the systematic choice related to the exercise of personal data after death with a 'personalistic model,'[25] which addresses both personality rights and personal data[26].

[21] Resta, *La "morte" digitale*, cit., at 894.

[22] Cinque, *La successione nel "patrimonio digitale"…*, cit., at p. 646.

[23] S. Delle Monache, *Successione* mortis causa *e patrimonio digitale*, *Nuova giur. civ. comm.*, 2, 2020, p. 460, at 460.

[24] In particular, Article 9, III, d.lgs. 196/2003, on similar model to the previous Article 13, III, l. 675/1996. This aspect is brought out by S. Stefanelli, *Destinazione* post mortem *dei diritti sui propri dati personali*, *MediaLaws*, 1, 2019, pp. 136-147.

[25] Resta, *La successione nei rapporti digitali e la tutela post-mortale dei dati personali*, *Contratto e impresa*, 1, 2019, at 89 and 104, where it is emphasized the distinction between this approach and two other models, defined as 'succession model' (which is based on a proprietary approach to immaterial goods of the individual and seeks to adapt the traditional succession law to the reality of the digital economy) and as 'contractual autonomy model' (which underlines the trend to develop computer models that help the data subject in making a conscious choice over the fate of her digital 'traces' after death).

[26] Resta, *La successione nei rapporti digitali…*, cit., at pp. 94-95.

The above-mentioned consistency between the previous formulation and the current formulation – which does not lack of significant innovations – is confirmed by the explicit reference which the ruling makes to the thesis of the persistent exercise of the rights on personal data beyond the life of the individual[27]. According to this doctrine, some legal systems, including the Italian one, favor 'an extension of protection, attributing to relatives, heirs or other subjects the power to exercise the rights of the data subject after his/her death,'[28] creating a sort of permanence of the individual rights amongst those mentioned by the legal provision[29].

By accepting this position, the Court shows to move away from the most relevant European judicial precedent addressing both digital death and digital inheritance: the 2018 ruling of the German *Bundesgerichtshof* on the case concerning the request for access to the Facebook account filed by the parents and heirs of an underage girl who died after an accident in the Berlin subway[30]. Following the prevailing theory amongst scholars, the German Federal Supreme Court had affirmed the full inheritability of personal data, adopting a 'succession model' for the data governance of a deceased individual.

Instead, the approach adopted by the Court of Milan reflects the aforementioned 'personalistic model'.

The solutions offered by the two rulings come to the same conclusion, i.e. the recognition of the right to access to the personal data of the deceased by the plaintiffs, from a practical point of view. However, they diverge on a theoretical level. The first one embraces the thesis according to which legal relationships concerning intangible goods pertain to the asset of the deceased and can be inherited, consistently with the principle of universality of succession (§1922 BGB)[31]. Instead, the second one, through the application of Article 2-*terdecies* Data Protection Code, recognizes a sort of persistence (*Fortwirkung*) of the rights in question beyond the life of the natural person, without the legislator having clarified whether it constitutes a legitimacy *iure hereditatis* or *iure proprio*[32].

[27] Trib. Milano, ord. 10.02.2021, p. 4.

[28] Resta, *La successione nei rapporti digitali…*, cit., at p. 97.

[29] Delle Monache, *Successione* mortis causa…, cit., at p. 465; in the same sense, F. Zagaria, *Patrimonio digitale e successione* mortis causa, *De iustitia*, 2020.

[30] BGH, 12-7-2018, III ZR 183/17. For a detailed analysis of the case, see R. Mattera, *La successione nell'account digitale. Il caso tedesco*, *Nuova giur. civ. comm.*, 2019, I, pp. 703-708.

[31] Resta, *La successione nei rapporti digitali…*, cit., at p. 91.

[32] Resta, *La successione nei rapporti digitali…*, cit., at p. 99.

Scholars seem to favor the second interpretation and justify this approach by stressing that the problem of vacancy of entitlement of the legal relationship, to which the succession phenomenon normally responds, would not occur when dealing with digital resources[33].

In other words, according to the Italian legislation, the postmortem exercise of the rights on personal data, recognized to certain categories of subjects, represents a possible answer to the legal questions raised by new technologies with regard to the fate of digital assets after the data subject's death[34]. In addition, the provision, compared to the hypothesis of the 'succession model', potentially expands the number of those entitled to exercise the rights and, at the same time, restricts it, as it provides for more stringent requirements for the permanence of rights to occur. Finally, it needs to be stressed that the legislator limits the general principle of the possible postmortal exercise of the rights on personal data. Indeed, the second paragraph of Article 2-*terdecies* does not admit the exercise of the referred rights in the cases provided for by law or when the data subject has expressly prohibited it, enhancing private autonomy and selfdetermination.

Ultimately, it is also worth mentioning the relationship between the judicial decision and the debated issue of digital sovereignty[35].

Most relevantly, in the Italian case the access request was related to data stored in the cloud computing platform iCloud. From this perspective, the Italian case differs from the well-known case of the San Bernardino attack, with which the issue of access to personal data of a deceased person – also for reasons of public interest – emerged on a global scale[36]. In the latter case, access to the cloud had been granted, but not to the physical device.

---

[33] Delle monache, *Successione* mortis causa…, cit., at 468: "*sembra che, quando ci si collochi al di fuori del perimetro dei diritti patrimoniali del defunto, ciò che può residuare, in realtà, siano solo forme di tutela* iure proprio*, con legittimazione attribuita dalla legge o comunque da riconoscersi, secondo i principi, a determinati terzi in base, per lo più, al loro legame familiare con il* de cuius".

[34] As stated by Article 2-*terdecies* d. lgs. 96/2003, the categories are: the ones having a 'personal interest', the ones acting to protect the interested party, or the ones acting 'for family reasons worthy of protection'.

[35] For an early comment on this aspect, see M. Bassini-G. De Gregorio-O. Pollicino, *L'accesso ai dati post mortem su cloud: il commento all'ordinanza del Tribunale di Milano 2020/44578*, *federnotizie.it*, 5 March 2021, available at: <https://www.federnotizie.it/laccesso-ai-dati-post-portem-su-cloud-il-commento-allordinanza-del-tribunale-di-milano-2020-44578/> (last access, April 09, 2021).

[36] A full scrutiny of the case and of the questions raised can be found in M. Orofino, *FBI v. Apple: il caso è (forse) chiuso, ma le questioni di fondo rimangono apertissime*, *DPCE online*, 26/2, 2016, pp. 277-295.

Digital inheritance evokes the operational difficulties typical of disputes concerning digital goods and data generated by digital platforms. Specifically, cloud computing allows to access the synchronized material from anywhere, regardless of the physical storage location and data retention.

In the decision of the Court of Milan, no circumstances from the evidence revealed the place of storage of the requested data. Furthermore, the decision of the Court denied Apple's claim to impose data access conditions typical of the US legal system, but extraneous to the Italian legal system. The judge concluded that the Court should rely on the rules of the legal system 'before which the right is enforced'[37].

This case explains well why the planetary dimension of the 'silicon giants'[38] also involves the jurisdiction and the law to be applied in the specific dispute.

To summarize, the ruling of the Court of Milan allows an initial definition of a few questions related to the issue of postmortem governance of digital resources, by embracing the theory of the persistent exercise of rights on personal data after the death of the data subject. At the same time, the above-mentioned decision leaves other issues unsolved, especially those concerning the concrete ways through which individuals may dispose of their rights on personal data after their death as well as the role which digital platforms will (or will not) play in relation to those powers of disposal.

[37] Trib. Milano, ord. 10.02.2021, p. 6.

[38] As Stefano Rodotà used to describe "*i grandi soggetti economici che si identificano con la rete*" (Rodotà, *Il diritto di avere diritti*, cit., p. 414).

Andrea Vigorito

Government Access to Privately-Held Data: Business-to-Government Data Sharing. Voluntary and Mandatory Models

Abstract. Climate change, pandemics and urban planning are just a few of the societal challenges that an efficient exploit of data could allow the public sector to tackle. In this perspective, business-to-government (B2G) data sharing can benefit the social good and allow for better policy decisions. Nevertheless, the possibility for the public sector to access privately-held data remains mostly unexplored. This contribution aims to explore the possible evolution of B2G sharing models within the future systems of data governance by evaluating rationales to foster government access to privately-held data and by analysing some of the barriers that hinder this kind of exploitation. This essay then seeks to present models of B2G data circulation through which societal benefits and data sharing could be improved; specifically, it focuses on the options of voluntary and mandatory B2G data sharing and outlines concrete experiences of B2G data sharing between private entities and European local administrations.

Keywords: B2G data sharing – data governance – data access – voluntary data sharing – mandatory data sharing

1. *Introduction: Data Governance and B2G Data Sharing*

The central role that the circulation of data plays within the modern digital economy and, more broadly, in today's information society[1], has prompted scholars to examine various models of data governance[2]. This term generally "seeks to reflect how data is collected, processed, and

[*] This article was first published in *European Journal of Comparative Law and Governance*, 2022, pp. 1-22.

[1] M. Castells, *The Rise of the Network Society* (2d ed., Wiley-Blackwell 2010); for a recent analysis of the "informational capitalism", see S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* Public Affairs, 2019; on the topic, see also J. E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism,* OUP, 2019.

[2] Lastly, T. Scassa, *Designing Data Governance for Data Sharing: Lessons from Sidewalk Toronto*, in *Technology and Regulation*, 2020, pp. 44–56.

used"[3]. This view of data as a "medium of governance"[4] has even led some commentators to claim that "European data law is bound to become a form of meta-regulation of legal governance by and with data"[5].

After the paradigm shift from the proprietary model to the model in favour of accessibility to data[6], the issue of data governance – which constitutes a logical corollary of a "disrupted law"[7] – has recently been addressed by the European Commission. In February 2020, the Commission published a European strategy on data[8] that includes the "promotion of data sharing between companies and public administration (*business-to-government*) for the public interest"[9].

Unlike the flow of data from government to business (G2B), which

[3] S. Viljoen, *A Relational Theory of Data Governance*, in *Yale Law Journal* vol. 131(2), 2021, pp. 573-654.

[4] T. Streinz, *The Evolution of European Data Law*, in P. Craig and G. de Burca (eds), *The Evolution of EU Law* (oup, 3rd ed. 2021), pp. 902-936.

[5] *Ibid*.

[6] A conceptual shift that reflects Stefano Rodota's thought in S. Rodotà, *Il terribile diritto* (3rd ed., Il Mulino 2013) p. 463 ("Muta lo sguardo sulla proprieta […] si potrebbe dire che si passa da una proprieta «esclusiva» ad una «inclusiva» […] *Il discorso sull'esclusione viene tramutato così in quello sull'accessibilità*", emphasis added). This shift has been observed with regard to non-personal data as well. The process is described by J. Drexl, *Data Access and Control in the Era of Connected Devices. Study on Behalf of the European Consumer Organisation BEUC*, (beuc 2018). More generally, regarding the distinction between personal and non-personal data, some scholars caution about the (non) usefulness of this categorization: see M. Finck and F. Pallas, *They Who Must Not Be Identified - Distinguishing Personal from Non-Personal Data Under the gdpr*, in *International Data Privacy Law* 10(1) (2020) 11–36; cf. I. Graef, R. Gellert, M. Husovec, *Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation*, in *European Law Review* 44(5) (2020) 605–621.

[7] C. Twigg-Flesner, *Disruptive Technology - Disrupted Law? How the Digital Revolution Affects (Contract) Law*, in A. De Franceschi, *European Contract Law and the Digital Single Market* (Intersentia 2016).

[8] Commission, "A European strategy for data" (Communication) com(2020) 66 final, as a result of the previous Communications: Commission, "Building a European data economy" (Communication) com(2017) 9 final and Commission, "Towards a common European data space" (Communication) com (2018) 232 final. The strategy has started to be implemented with the recent 'package' of proposals, including the Data Governance Act, the Digital Markets Act and the Digital Services Act.

[9] Commission, "A European strategy for data" (n 9) 15. The promotion will be achieved on the basis of the evidence reported in European Commission (ed), Towards a European strategy on business-to-government data sharing for public interest: Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing (EU 2020).

has found specific regulation at the EU level[10], the analysis of the issue of access by public authorities to data held by private individuals (B2G) remains largely unaddressed[11].

The infrequent implementation of B2G data sharing models occurs due to a variety of factors. Firstly, private companies show an insufficient aptitude towards recognizing both a social and a commercial value to data (offer side). Secondly, the public sector itself does not appear technically equipped to operate data sharing models (demand side)[12]. Finally, even though the most widespread opinion highlights a direct correlation between the circulation of data towards the public sector and possible improvements in terms of welfare there is no lack of contrary views. These warn about the possibility that stimulating B2G data sharing can have adverse effects on the "efficiency of data driven markets and, consequently, of data driven innovation"[13].

Proceeding on the basis of this prevailing theory, this essay will analyse existing rationales and barriers to B2G data sharing (2.) and then evaluate possible models that could facilitate business to government data sharing (3.). Furthermore, the article takes into consideration a few concrete experiences of B2G data sharing practices between private companies and European local administrations in order to better illustrate the operational

[10] Parliament and Council Directive 2019/1024/EU of 20 June 2019 on open data and the re-use of public sector information [2019] oj L172/56 (psi Directive).

[11] This has been pointed out, in one of the few studies on the topic, by H. Richter, *The law and policy of government access to private sector data ('B2G data sharing')*, in Bundesministerium der Justiz und für Verbraucherschutz, Max-Planck-Institut für Innovation und Wettbewerb (ed), *Data Access, Consumer Interests and Public Welfare* (1st ed. 2021) 529 <https://doi.org/10.5771/9783748924999-529> retrieved 29 April 2021. In the same sense, A. Alemanno, *Data for Good. Unlocking Privately-Held Data to the Benefit of the Many*, in *Eur J Risk Regul, vol.* 9(2), 2018, 183–191.

[12] Alemanno, *Data for Good. Unlocking Privately-Held Data to the Benefit of the Many*, cit. p. 189; see also European Commission (ed), Towards a European strategy on business-to-government data sharing for public interest, cit. in Chapter iv. In addition to that, the latest version of the Data Governance Act's proposal (that will be further analysed in section 3.1) has added the Article 14a to the original text, which states: "Member States may have in place organisational and/or technical arrangements to facilitate data altruism. In support of this Member States may define national policies for data altruism".

[13] N. Elkin-Koren and M. Gal, *The Chilling Effect of Governance-by-Data on Data Markets*, in *The University of Chicago Law Review*, vol. 86, 2019, pp. 403–431. Also, for a critical analysis of the data sharing regulatory model in the specific sector of financial industry, see O. Borgogno and G. Colangelo, *The data sharing paradox: BigTechs in finance*, in *European Competition Journal*, vol. 16, 2020, pp. 492–511.

data sharing options (4.). In the last section, some conclusions regarding the future evolution of data governance and B2G data sharing will be drawn (5.).

From a methodological point of view, the study will examine how data sharing practices operate both in theory and in practice.

It will begin by analysing rationales and barriers to business-to-government data sharing mainly in a socio-economic perspective with the intent to clarify the possible benefits deriving from data sharing practices. Furthermore, the limitations needed in a B2G data sharing system to avoid potential legal challenges inherent to fundamental rights will also be taken into account.

The study will then focus more specifically on the possible data sharing models. On a theoretical level, the difference between voluntary or mandatory methods will be outlined by giving special attention to the legal questions arising from the introduction of the concept of "data altruism" proposed by the Data Governance Act. From a practical point of view, consideration will be given to multilateral partnerships (between one municipality and several private companies or vice versa) as an example of data sharing practices, since such an approach is considered more functional to envisage the possible development of the European data governance system.

2 *Rationales: Identifying Social Benefit Stemming from Data Access*

A fundamental feature of data is complementarity: indeed, the value of data derives from its use and reuse by a plurality of subjects that combine the same data to pursue different ends[14]. This mechanism occurs by virtue of the non-rivalrous nature of data[15], which therefore allows it to be exploited simultaneously by several subjects without being exhausted.

In this sense, a sub-optimal level of data sharing would produce an equally sub-optimal level of exploitation of data, from the point of view of economic efficiency. Although the benefits arising from a correct

[14] Generally, the economic Value is added, together with 'veracity', to the "three features [that] are key to the technical understanding of big data: volume, velocity and variety (the so-called '3 Vs')", as stated by J. Drexl, *Designing competitive markets for Industrial Data – Between Propertisation and Access*, in *JIPITEC* 8, 2017, 257–292, p. 264.

[15] For further analysis, C. I. Jones, C. Tonetti, *Non-rivalry and the economics of data*, in Stanford Graduate School of Business Working Paper, 2019, p. 371

circulation of data seem clear, it is not easy to systematically assess them because due to the above-mentioned complementarity of data: it is only through the aggregation of data originating from different sensors or collected by different subjects that its actual value can emerge[16].

The fact that private tech companies and platforms "have amassed more data about people and their behaviour, health, markets and networks"[17] than governments does not allow the data governance system to reach a first best efficiency level of exploitation of data. In addition to that, the distance in terms of power and knowledge between consumers and large tech companies give rise to a "data asymmetry in society"[18], which must be remedied.

In this perspective, by facilitating data sharing to the public sector, relevant social benefits could be attained[19]. In particular, studies have thus far focused on aggregated information defined as "data of general interest"[20]. Data of general interest or data that can be used fruitfully, thanks to its complementarity, by the public sector is often collected by private companies. Access to such data would allow to repurpose and combine "private intent data" with "public intent data"[21] and produce positive effects on many levels. For instance, mobility data can help

[16] In a dynamic that resembles the well-known Arrow's information paradox (which affects data as well), described in K. Arrow, "Economic Welfare and Allocation of Resources for Invention", in National Bureau of Economic Research (ed), *The Rate and Direction of Inventive Activity: Economic and Social Factors* (pup 1962) 609, 615: "there is a fundamental paradox in the determination of demand for information; its value for the purchaser is not known until he has the information, but then he has in effect acquired it without cost".

[17] J. Shkabatur, *The Global Commons of Data*, in *Stanford Technology Law Review* 22 (2019) 354–411, 357.

[18] Alemanno, *Data for Good. Unlocking Privately-Held Data to the Benefit of the Many*, cit., p. 185.

[19] S. G. Verhulst, A. Young. *How the Data That Internet Companies Collect Can Be Used for the Public Good*, in *Harvard Business Review*, 23 January. Retrieved 29 April 2021, <https://hbr.org/2018/01/how-the-data-that-internet-companies-collect-can-be-used-for-the-public-good>.

[20] B. Pailhes, *How to define and regulate "data of general interest"?*, in *Enjeux numeriques*, 2018. Retrieved 26 December 2021 <http://www.annales.org/enjeux-numeriques/2018/resumes/juin/09-enresum-FR-AN-juin-2018.html>; Richter, *The law and policy of government access to private sector data ('B2G data sharing')*, cit. *passim*.

[21] World Bank, *World Development Report 2021: Data for Better Lives*, Washington, DC: World Bank. doi:10.1596/978-1-4648-1600-0, 2021, p. 54 in which "public intent data" are described as "data collected with the intent of serving the public good by informing the design execution, monitoring, and evaluation of public policy, or through other activities".

monitor public health, including infectious diseases[22].

Additionally, data obtained from cell phones or social media has been used to improve road safety or to understand traffic safety culture[23]. Data not collected by national governments is also useful, not only to support or compare policy priorities (such as financial inclusion[24]), but also to verify how a given policy intervention is perceived or how it could be fixed or improved[25].

In summary, it is argued that such an approach – which favours the combination of private and public sector data – could benefit both current (urban planning, public health, transport, public safety, …) and future public tasks (scoring algorithms, smart cities)[26].

Applications of this kind of reasoning can be found in the context of public services, including future policy decisions and their related decision-making process. On the one hand, the data detected by cell phone sensors would allow for an analysis of traffic conditions, improve the management of traffic flows or public transport. On the other hand, it would allow authorities to choose the correct policy option to address specific needs by, for instance, studying the pollution that traffic produces in cities.

Concrete examples could be identified in the program developed by Vodafone[27] which allows public authorities to manage trends in population flows or to control epidemics and in the European initiative[28] created with the aim of improving road safety by allowing vehicles to share

[22] We have been witnessing this kind of exploitation of data with the Covid-19 pandemic. For a comprehensive examination of implications for data protection of tracing apps, see E. Poillot et al., *Data protection in the context of covid-19. A short (hi)story of tracing applications*, RomaTrE-Press, 2021.

[23] World Bank, *World Development Report 2021: Data for Better Lives*, cit., pp. 129–130.

[24] *Ibid*.

[25] Alemanno, *Data for Good. Unlocking Privately-Held Data to the Benefit of the Many*, cit., p. 184.

[26] Richter, *The law and policy of government access to private sector data ('B2G data sharing')*, cit., p. 536, where the Author makes the cited distinction between public tasks and new public tasks.

[27] See N. Rana and U. Majmudar. *Data can be a force for social good: Nuria Oliver, Vodafone*, 2018. The Economic Times, 4 October. Retrieved 29 April 2021, <https://economictimes.indiatimes.com/blogs/ResponsibleFuture/data-can-be-a-force-forsocial-good-nuria-oliver-vodafone/>; the initiative is also analysed in International Data Corporation and the Lisbon Council (2016), Opening Up Private Data for Public Interest, European Data Market Study <https://datalandscape.eu/sites/default/files/report/Story_1_New_format.pdf> 22–25, as case study n. 3.

[28] Data Task Force, on Data for Road Safety website <https://www.dataforroadsafety.eu>, retrieved 29 April 2021.

relevant information[29].

At the same time, the risks of promoting an intensive data sharing approach cannot be overlooked. Facilitating data sharing for public-interest purposes must be carried out without encroaching on of fundamental rights. The risks that come with an excessive or incorrect use of data are well known and addressed by scholars[30]. Firstly, data collection itself creates the general risk of privacy incursions which can jeopardize individuals' dignity and self-determination[31]. Secondly, governmental access to data could lead to the increase of mass (self-)surveillance, already amplified by the advent of the Internet of Things[32]. Thirdly, an incorrect use of data, because of the intimate relation between data and algorithmic systems, is now able to generate reproduction, stabilization or amplification of social and economic inequality[33].

Consequently, it is crucial to determine the correct safeguards and to

[29] Both the examples are cited in European Commission (ed), *Towards a European strategy on business-to-government data sharing for public interest*, cit., p. 15.

[30] Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, cit.; Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, cit.; K. Crawford, *Atlas of AI* (yup 2021); D. Lyon, *The Culture of Surveillance: Watching As a Way of Life*, Polity Press, 2018; F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, HUP, 2015; S. Zuboff, *Big other: surveillance capitalism and the prospects of an information civilization*, in *Journal of Information Technology*, vol. 30(1), 2015; cf. also OECD, Enhancing *Access to and Sharing of Data* (2019) retrieved 29.12.2021 <https://www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en>.

[31] Viljoen, *A Relational Theory of Data Governance*, cit.; J. Cohen, *What Privacy is For*, in *Harv L Rev*, vol. 126, 2013, pp. 1904–1933; M. Hildebrandt, *Privacy As Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, in *Theoretical Inquiries of Law*, vol. 20, 2019, pp. 83–121. More broadly, see P. Schwartz, *Internet Privacy and the State*, in *Connecticut Law Review*, vol. 32, 2000, 815–859.

[32] Understood as "the intentional or consensual creation of mass information about oneself through electronic tracking or other means"; for this definition and the implications of IoT on privacy, see S. I. Friedland, *Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things Is Changing the Face of Privacy*, in *W Va L Rev*, vol. 119, 2017, 891–914. Also, for a comparative analysis on surveillance and fundamental rights, see F. H. Cate, J. X. Dempsey (eds), *Bulk Collection: Systematic Government Access to Private-Sector Data* (OUP 2017).

[33] Crawford, *Atlas of AI,* cit.; C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown Pub, 2016; D.K. Citron, F. Pasquale, *The Scored Society: Due Process for Automated Predictions*, in *Washington Law Review* vol. 89, 2014, 1–33; S. Rodota, *Protezione dei dati e circolazione delle informazioni*, in Id., *Tecnologie e diritti* (2021) 43–96.

find an adequate balance between the interests at stake[34].

To this end, the principles elaborated by the European Commission for business-to-government data sharing must be central to discussions on the growth of data sharing between private entities and public authorities, no matter the model of data governance that is adopted. In order for the data sharing activities to be compatible with the fundamental rights involved, principles on business-to-government data sharing, which place clear limits to the extent of data sharing practices, have been set out and recently revised[35].

More specifically, the revised principles include: a) proportionality in the use of private-sector data; b) data-use limitation; c) risk mitigation and safeguards; d) compensation; e) non-discrimination; f) mitigate limitations of private-sector data; g) transparency and societal participation; h) accountability; i) fair and ethical data use[36].

The major legal challenges arising from B2G data sharing are addressed by some of these principles.

The "proportionality principle" require a verifiable public interest and includes a balancing test between the chosen public interest and the interest of other stakeholders. In this way, fundamental rights of individuals find a first safeguard in the requested balancing activity.

Additionally, the notion of "data-use limitation"[37] involves relevant legal aspects: indeed, the use of data is limited for one or several public-interest purposes which, once identified, should be clearly specified; furthermore, the data sharing agreements should respect existing legislation, "including privacy, intellectual property and database laws, and contractual obligations to which private and civil-society organisations may be bound"[38]. In particular, even though it is common for digital data not to meet the criteria for the protection offered by copyrights and database rights, whenever an intellectual property right protects the data,

[34] The World Bank, *Unraveling Data's Gordian Knot: Enablers & Safeguards for Trusted Data Sharing in the New Economy*, 2020, p. 25.

[35] The listed principles are the updated version by European Commission (ed), *Towards a European strategy on business-to-government data sharing for public interest*, cit., pp. 79–86, that contain a revised version of the principles set out by the European Commission in 2018 (Commission, "Towards a common European data space" com (2018) 232 final).

[36] Even though the study will follow the titles proposed by the Expert Group, the same considerations can be made with regard to the original version of the principles.

[37] The Expert Group suggested to change the former title 'purpose limitation' because it "is more a privacy principle".

[38] European Commission (ed), *Towards a European strategy on business-to-government data sharing for public interest*, cit., p. 81.

it represents a limit that data sharing agreements cannot circumvent.

Finally, a responsible approach is requested both from public authorities in the use of data and from private entities in the collection of information in accordance with the "risk mitigation principle". Indeed, this principle extends its effectiveness not only to activities of the public sector, but also to *ex ante* operations made by private collectors of data. Fundamental rights including privacy, data security, non-discrimination must be safeguarded in each phase of the process. This can be regarded as a measure that prevents a distortion of the actions of businesses and avoids a more irresponsible collection of data that would increase the level of the so-called "data extractivism"[39].

The principles elaborated by the Commission can help in designing better data sharing agreements; nonetheless, the current "volume of B2G data transactions may be insufficient from a social welfare perspective"[40] since it is possible to observe market failures that currently impede the use of B2G sharing models. Other barriers – on both an economic and governance level – preclude B2G data sharing.

From a purely economic point of view, scholars identify three main obstacles:[41] a) monopolistic data markets, which allow companies in a privileged position to request a high price for access to the data they hold; b) high transaction costs and perceived risks, which concern both, *ex ante*, the costs inherent in the research and preparation of an agreement with the other party, and, *ex post*, the risks relating to the quality of the data and their technical implementation; c) lack of incentives, since many companies may believe that data sharing can only have negative effects, which should therefore be addressed, for example, through forms of compensation[42].

On a more general level of governance, four different categories of obstacles to data sharing can be causes for concern: organisational, cultural, techno-operational and governance related[43]. Organizational

[39] E. Morozov, *There is a leftwing way to challenge big tech for our data. Here it is*, The Guardian, (retrieved 26 December 2021, <https://www.theguardian.com/commentisfree/2018/aug/19/there-is-a-leftwing-way-to-challenge-big-data-here-it-is>).

[40] B. Martens, N. Duch-Brown, *The economics of Business-to-Government data sharing*, 2020, jrc Digital Economy Working Paper 2020–04, 12.

[41] *Ibid*.

[42] European Commission (ed), *Towards a European strategy on business-to-government data sharing for public interest*, cit., p. 39, identified four types of compensation: free of charge; marginal costs for dissemination; marginal costs for dissemination + fair return on investment (roi); market price.

[43] European Commission (ed), *Towards a European strategy on business-to-government*

challenges relate to the investments that the provider should make to manage this type of operations. Cultural obstacles are the result of a lack of data sharing culture. From a techno-operational point of view, the limited availability of systems that guarantee security and privacy of data appears to be the central issue. Governance issues arise primarily from the absence of an adequate legal framework.

Against this backdrop, any legal reform should try to take into consideration the previously mentioned aspects in order to encourage a culture of data sharing and identify a data governance model that does not give rise to technical or economic inefficiencies or to any violation of fundamental rights. Therefore, the analysis of the possible models of data sharing is necessary to understand in which ways data sharing can be shaped in accordance with these legal, economic and governance principles.

3 *Models of Data Sharing*

After having identified the positive effects which can be fostered by access to data in the previous section, the study will now focus on suitable methods to access privately-held data.

Firstly, it is possible to make a distinction between solutions that contemplate models of voluntary data sharing and models of non-voluntary data sharing without, however, necessarily conceptualizing these models as mutually exclusive.

As the European model seems to suggest, the two solutions should indeed be able to coexist in a system that provides for both possibilities[44].

Alternatively, a middle ground solution could be to incentivize voluntary B2G data sharing, without resorting to compulsory access[45]. Yet, it is important to underline that, since mandatory access rules and voluntary based data sharing models are two solutions that lie at the opposite ends of

data sharing for public interest, cit., p. 25.

[44] As reflected in the "European strategy on data" (n 9). The direction taken will be confirmed or disregarded by the future Data Act in 2022.

[45] Martens and Duch-Brown, *The economics of Business-to-Government data sharing*, cit., pp. 5–6: "facilitate voluntary B2G operations without mandating them". For a further option, see Shkabatur, *The Global Commons of Data*, cit., pp. 399–402, where the Author invokes the "public utility doctrine", identifying data platforms as *de facto* "public utilities", as they meet the double condition of being considered a "natural monopoly" and being "affected with public interest".

the spectrum, the system offers "less interventionist instruments to foster data access (e.g., incentives, reduction of transaction costs or soft law approaches)"[46]. More specifically, in regard to the incentives, for instance, they could be "direct, i.e., monetary, or indirect, i.e., reputational (e.g., as part of corporate social responsibility programmes)"[47]. In addition to that, intermediaries play a key role in the growth of data sharing activities between private entities and public authorities: they are indeed essential to increase trust between the parties and reduce transaction costs[48].

Therefore, the next sections analyse the main aspects of the prospected data sharing solutions, on a voluntary or compulsory basis.

3.1 *Voluntary B2G Data Sharing and Data Altruism*

In line with the spread of a culture of digital philanthropy[49], the Data Governance Act[50] is the most recent example of the use of a voluntary access method, a development that has stimulated scholarly discussion. The proposal envisages an entire chapter (Chapter iv) dedicated to what is defined as "data altruism"[51], which would allow legal or natural persons to voluntarily transfer the data they collect to the public sector. By "data altruism", the European Commission's proposal means "data voluntarily made available by individuals or companies for the common good"[52]. Specifically, Recital no. 35 identifies the following "objectives of general interest", relevant to non-personal data: "healthcare, combating climate

[46] Richter, *The law and policy of government access to private sector data ('B2G data sharing')*, cit., p. 537.

[47] Martens and Duch-Brown, *The economics of Business-to-Government data sharing*, cit., p. 5.

[48] In general, about the role of intermediaries in the digital economy, see H. Richter and P. Slowinski, *The Data Sharing Economy: On the emergence of New Intermediaries*, in *IIC - International Review of Intellectual Property and Competition Law* vol. 50, 2019, 4–29.

[49] M. Taddeo, *Data Philanthropy and Individual Rights*, in *Minds and Machines* 27, 2017, 1–5; cf. R. Kirkpatrick, *A new type of philanthropy: donating data*, in *Harvard Business Review*, 21 March, 2013. Retrieved 29 April 2021, <https://hbr.org/2013/03/a-new-type-ofphilanthropy-don>.

[50] Commission, "Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)" com(2020) 767 final. On the 1st of October 2021, the Council of the European Union reached agreement about the text of the proposed European Commission Data Governance Act.

[51] A view that is coherent with the need of solidarity (in this context, digital solidarity) expressed by S. Rodotà, *Solidarietà. Un'utopia necessaria,* Editori Laterza, 2014.

[52] Commission, Proposal for Data Governance Act, cit. p. 8.

change, improving mobility, facilitating the development, production and dissemination of European statistics or improving the provision of public services[53]".

To concretely implement this data sharing model, the Data Governance Act proposal also contains provisions regarding a "European data altruism consent form"[54] and the requirements, especially in terms of transparency and data protection, for the registration of "data altruism organizations".

On the one hand, scholars have stated that the new concept of "data altruism consent" could be seen both as "another requirement for data sharing [and as] an opportunity to harmonize legislation across the EU Member States and thereby ease data sharing at least within the EU"[55]. The Commission further specifies that "[s]uch a form [of consent] should contribute to additional transparency for data subjects that their data will be accessed and used in accordance with their consent and also in

[53] *ibid*., 20. The previous version, modified by the Council, was referring to them as "purposes" of general interest and included: "healthcare, combating climate change, improving mobility, facilitating the establishment of official statistics or improving the provision of public services". The new version of the proposal also adds to the last part of the Recital that: "In order to achieve this objective, Member States could have organizational or technical arrangements in place, which would facilitate data altruism. Such arrangements could include the availability of easily useable tools for data subjects or data holders for giving consent or permission for the altruistic use of their data, the organization of awareness campaigns, or a structured exchange between public authorities on how public policies benefit from data altruism (e.g., improving traffic, public health, combating climate change). In support of this, Member States could also define national policies for data altruism. Data subjects should be able to receive compensation related only to the costs they incur making their data available for objectives of general interest".

[54] Article 22, which states: (1) In order to facilitate the collection of data based on data altruism, the Commission may shall adopt implementing acts establishing and developing a European data altruism consent form, after consultation of the European Data Protection Board, and duly involving relevant stakeholders. The form shall allow the collection of consent across Member States in a uniform format. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 29(2). (2) The European data altruism consent form shall use a modular approach allowing customization for specific sectors and for different purposes. (3) Where personal data are provided, the European data altruism consent form shall ensure that data subjects are able to give consent to and withdraw consent from a specific data processing operation in compliance with the requirements of Regulation (EU) 2016/679. (4) The form shall be available in a manner that can be printed on paper and is easily understandable and read by humans as well as in an electronic, machine-readable form".

[55] M. Shabani, *The Data Governance Act and the EU's move towards facilitating data sharing*, in *Molecular Systems Biology* vol. 17, 2021, p. 2.

full compliance with the data protection rules"[56]. It therefore seems clear that the rationale behind this measure aligns with the general intent of empowerment of individuals[57].

In this direction, compliance to the gdpr requirements for giving or withdrawing consent is explicitly required when dealing with personal data. This condition should also ensure protection to consumers who may misunderstand the notion of "data altruism", whose concept – especially with regard to the public-interest purposes or objectives – needs to be better specified for it risks being misused to influence consumers and create wrong perceptions[58].

Furthermore, the debate on consent has been influenced by the changes to the proposal made by the Council. In particular, the new Article 19a specifies the safeguards to individuals' fundamental rights that codes of conduct shall guarantee, including information related to "the use of data, the tools for the giving and withdrawal of the consent, and the measures taken to avoid misuse of the data shared with the data altruism organisations".

On the other hand, the "data altruism organisations" are intended to act as intermediaries between the data provider and the receiving public sector authority, thereby increasing the confidence of the parties to enter into such a negotiation.

Trust, together with security and transparency, does indeed represent a key factor of "infraethics"[59], whose principles are "likely to facilitate morally good actions"[60] and of which data philanthropy itself is believed to be a part of[61]. Taking these aspects into consideration and increasing a data sharing culture is a prerequisite for building an inclusive and open information society[62]. Nevertheless, the latest version of the proposal

[56] Commission, Proposal for Data Governance Act, cit., Recital 39.

[57] Shabani, *The Data Governance Act and the EU's move towards facilitating data sharing*, cit.

[58] Beuc, *Data Governance Act Position Paper*, 2021, p. 7: "'data altruism' is a problematic term which can be misused to unduly influence consumers. The 'altruistic' element might be used to nudge consumers into a choice and behaviour which may not be justified depending on the circumstances".

[59] The term, introduced by L. Floridi, *Distributed morality in an information society*, in *Science and Engineering Ethics* vol. 19(3), 2013, 727–743, p. 738, refers to "not-yet-ethical framework of implicit expectations, attitudes, and practices that can facilitate and promote moral decisions and actions".

[60] Taddeo, *Data Philanthropy and Individual Rights*, p. 3.

[61] *Ibid*.

[62] For the notion of "inclusiveness" in the information society, specifically regarding smart cities, see T. Scassa, *Keynote Address from Go Open Data 2019 Conference*,

specifies that: "[r]egistration as a recognised data altruism organisation should not be a precondition for exercising data altruism activities"[63].

However, although praised, the effort towards the provision of voluntary data sharing models has been considered still insufficient, sectoral, experimental and not sustainable in the long run, not only because of the lack of sharing culture, but especially due to the absence of adequate data governance structures both in private companies and in public institutions[64]. These aspects raise the question of "how to move from this emerging, sector-to-sector, voluntary approach to a more universal, sustainable and accountable data sharing model (or models)"[65]. The data altruism system designed by the Data Governance Act proposal seems to begin to answer this question.

3.2 *Mandatory B2G Data Sharing*

Compulsory access lies at the opposite end of the spectrum. It must be stressed that forcing access, under certain conditions, to data held by companies is a solution that constitutes an *extrema ratio* and requires adequate justification since it represents an encroachment on fundamental rights[66].

According to the European Commission, "the general principle shall be to facilitate voluntary data sharing" and "only where specific circumstances so dictate, access to data should be made compulsory, where appropriate under fair, transparent, reasonable, proportionate and/or non-discriminatory conditions"[67]. In other terms, a mandatory regulatory

6 May 2019. Retrieved 20 April 2021, <https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=307:keynote-address-from-go-open-data-2019-conference&Itemid=80>.

[63] Commission, Proposal for Data Governance Act, cit., Recital 36.

[64] Alemanno, *Data for Good. Unlocking Privately-Held Data to the Benefit of the Many,* cit., p. 187.

[65] *Ibid*., 8.

[66] Richter, *The law and policy of government access to private sector data ('B2G data sharing')*, cit., p. 537; furthermore, it has to be noted that some sector-specific disciplines already include mandatory access models in B2B relations, such as Parliament and Council Regulation (ec) No. 1907/2006 of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (reach) [2006] or Parliament and Council Regulation (ec) No 715/2007 of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information [2007].

[67] Commission, *A European strategy for data*, cit., p. 13; in particular, "data access

framework could stand, for instance, when "a private data supplier faces strong negative incentives to participate in a B2G data transfer, despite the fact that the public interest or social welfare impact of an operation would considerably exceed the private costs of the supplier"[68].

According to scholarly research into the topic, mandatory access rules should be designed on a horizontal level and must include five fundamental aspects: purpose, beneficiaries, obliged parties, relevant data, and modalities of access[69].

On the teleological level, identifying the purpose of forced access requires a definition of what is meant by 'public interest', as is its prerequisite. As regards the parties, 'beneficiaries' should be understood as the public authorities, that should be identified on a case-by-case basis, while 'obliged parties' should be understood to be private companies, such as "data holders"[70]. On the objective dimension, the type of data to be collected may depend on the purpose of the access, distinguishing – in any case – raw data, pre-processed data, processed data and data-driven insights. Finally, the 'modalities of access' concern both the technical tools that can be used for the transfer of data and the compensatory profiles that affect such transactions.

In light of the above, the first and main aspect that has to be taken into account when dealing with the hypothesis of mandatory access rules remains the 'public interest purpose'[71]. Due to the strict conditions and justifications needed for such a restriction, the fact that there must be a

right should only be sector-specific and only given if a market failure in this sector is identified/can be foreseen, which competition law cannot solve. The scope of a data access right should take into account legitimate interests of the data holder and needs to respect the legal framework" (footnote 39).

[68] Martens, Duch-Brown, *The economics of Business-to-Government data sharing*, cit., p. 21.

[69] Richter, *The law and policy of government access to private sector data ('B2G data sharing')*, cit., pp. 542–550, asking these five questions: "what for, for whom, against whom, to what and how?".

[70] About the difference between "data holders" and "data owners", see Drexl, *Data Access and Control in the Era of Connected Devices*, cit. 29; cf. D. Kim, *No one's ownership as the status quo and a possible way forward: A note on the public consultation on Building a European Data Economy*, in *Journal of Intellectual Property Law & Practice* vol. 13, 2018, 154–165, p. 158 ("*The quotation marks indicate that the term 'data owners' does not imply ownership in the legal sense*").

[71] To support this statement, see European Commission (ed), *Towards a European strategy on business-to-government data sharing for public interest*, cit., p. 48, in which the table that depicts 'Business-to-Government data sharing for the public interest: step by step' interrupts the process at the first step if a public interest purpose doesn't occur.

public interest purpose in order to allow forced access to privately-held data cannot be overlooked.

Nevertheless, to identify what is meant by 'public interest' or to define the scope of application of a legislative framework that includes the notion of 'public interest' is not an easy task, given that it may differ between sectors and between various social-cultural contexts. Therefore, finding the correct definition of this notion represents a central issue in the elaboration of mandatory B2G data sharing models[72].

4 *Case Studies: European Local Administrations*

Within the aforementioned B2G data sharing context, some European municipalities have been implementing data sharing practices. Coherently with the opinion that "the impact of *local* institutional frameworks is particularly strong in the regulation of emerging digital technologies"[73], a brief description of certain European local administrations' concrete experiences will contribute to highlight the existing informational asymmetry between companies and public authorities and to examine solutions through which the issue has been addressed until now.

As the case studies will show, the current status of B2G data sharing needs to be analysed by underlining some aspects that may differ from one experience to another.

A first difference relates to the sector and the type of data: mobility data sharing seems to be more mature than energy data sharing[74].

A second aspect of interest is the fact that some cities lack a technical structure that would allow them to better exploit the data which they are able to harvest, while other municipalities face barriers to obtaining data in the first place.

[72] This aspect has been pointed out with regard to the "data altruism" concept as well, as stated in beuc, *Data Governance Act Position Paper*, cit., p. 8.

[73] G. Resta, *Data and Territory. The impact of the "local" in the regulation of digital technologies and algorithmic decision-making*, in *Essays in honour of Mads Adenas*, (emphasis added), where it is also stressed that "an inherent tension may be observed between technologies that are *unterritorial* by nature and regulatory patterns which are inherently *local*".

[74] European Commission, Event Report, *Business to Government (B2G) data sharing workshop – 5th and final workshop*. Retrieved 12 August 2021, <https://digital-strategy.ec.europa.eu/en/library/business-government-b2g-data-sharing-workshop-5th-and-final-workshop>.

Furthermore, each administration adopts different data sharing techniques. In particular, commentators have identified four operational models: a) data donorship, in which companies share data on a voluntary basis; b) public procurement of data, which is based on the purchase made by the public authority of a specific set of privately-held data; c) data sharing partnerships, through which local administrations and companies act in a collaborative way by sharing data and cooperating on the basis of mutual interests; d) tender obligations that consist of contractual clauses which oblige the supplier of a given service to share their data with the local administration[75].

Nevertheless, B2G data sharing practices will also show that some sectors are governed by mandatory rules imposed by national law.

Finally, local administrations' experiences prove that current business-to-government data sharing practices are favouring bilateral relationships. Indeed, instead of building a common data space or large partnerships involving several actors, data sharing is often based on a bilateral transaction between one municipality and one company. However, more benefits could be reached by implementing multilateral partnerships, both as partnerships consisting of a single municipality operating with several private companies and as partnerships including a network of cities[76]. The

[75] The categorization is made by M. Micheli, *Accessing privately held data: Public/private sector relations in twelve European cities*, Paper presented at Data for Policy 2020 Zenodo. Retrieved 12 August 2021, <https://doi.org/10.5281/zenodo.3967044>. The study was based on semi-constructed interviews with the innovation/data managers of twelve European local administration. Another remarkable aspect underlined by the study is that of *data sovereignty*: "respondents are wary in buying data through *public procurement*, both because that would place them in a dependent position (economically), and because there is a lack of transparency regarding privately held data quality as well as limited possibilities for controlling how it is formatted and used. To preserve control, some respondents envision a form of collective bargaining to strike better deals when acquiring data, but most often they look towards other modes of access. The best ways to keep control of data include establishing actual collaborative relations (co-creation) through *data partnerships* with private companies and, when possible, including *obligations clauses in tender contracts* with suppliers. Some of the strategies proposed to maintain control are collective efforts in which cities join forces for this cause: from collective bargaining, to develop a common contractual framework to use with businesses for tenders or partnerships. These tactics could indeed help to level the playing field, lessening the inequalities described above, and increasing cities' strength in demanding access to privately held data with a public interest".

[76] As highlighted by M. Micheli in European Commission, Event Report, *Business to Government (B2G) data sharing workshop – 5th and final workshop*. Retrieved 12 August 2021, <https://digital-strategy.ec.europa.eu/en/library/business-government-b2g-datasharing-workshop-5th-and-final-workshop>.

exchange of best practices between territories would not only allow a better understanding of the possible data sharing methods currently used by the public sector, but it could also facilitate a more standardised approach and counterbalance the asymmetry of power that exists between small local administrations and large national or international companies[77].

In light of these considerations, the paper will now analyse a few examples of B2G data sharing practices based on multilateral cooperation.

In this section, an empirical methodology is used with the intend to show how municipalities are dealing with B2G data sharing when multiple stakeholders are involved. To this end, the following case studies have been selected by taking into account techniques adopted in different countries and by including not only well-known smart cities, but also different and smaller or less populated ones.

As anticipated, it seems that adopting multilateral partnerships would facilitate the implementation of large common data spaces and it would allow for the exchange of data between several actors. Therefore, understanding what strategies are used in accessing privately-held data becomes crucial for the future development of data sharing methods.

In particular, the study will examine not only the aim of data sharing agreements, which must act in compliance with a public-interest purpose criterion, but it will also specify which instruments are used to design mandatory access rules (if they are required by law or by contractual agreements).

4.1 *Rennes*[78]

According to French law[79], since 2015 energy suppliers have to share

[77] Marion Glatron (Directrice deleguee Innovation et Smart City Rennes Metropole), *Sharing data at a local scale for Energy Transition*, 9th June 2021, presentation given at B2G data sharing in energy – 3rd B2G Data Sharing Workshop. Retrieved 13 August 2021, <https://digitalstrategy.ec.europa.eu/en/library/b2g-data-sharing-energy-3rd-b2g-data-sharing-workshop>.

[78] B2G data sharing practices in Rennes have been illustrated by Marion Glatron (smart cities and innovation director, Rennes Metropole) in European Commission, Event Report, "B2G data sharing in energy – 3rd B2G Data Sharing Workshop", Retrieved 13 August 2021, <https://digitalstrategy.ec.europa.eu/en/library/b2g-data-sharing-energy-3rd-b2g-data-sharing-workshop>.

[79] Article 173-vi of the French Energy Transition for Green Growth Act; see also Article 29 of Law No. 2019–1147 (Energy-Climate Law) of November 8th 2019 and its implementing decree published on May 27th 2021 (retrieved 13 August 2021, <https://

(on a 'comply or explain' basis)[80] their data with public authorities[81]. This mechanism allowed the public sector to access data related to energy production, energy consumption, and renewable energy. However, the data flow was still insufficient to improve the local decision-making process. Therefore, the city of Rennes started a data sharing project on a local scale which included Rennes Metropole, urban planning agencies and energy distributors. The energy related real-time data obtained through this collaboration allowed for a precise mapping of the city, including buildings' characteristics (heights, volume, age), roads, local urban zoning, and vegetation density.

This multilateral partnership between a single municipality and multiple private players shows that a model which combines legally mandated data sharing and collaboration between multiple actors is possible and facilitates data analysis based on a better quality of data.

4.2 *Barcelona*[82]

Another model of data sharing based on a cooperation agreement can be found in Barcelona. Barcelona City Council, Direccion General de Trafico and Mobileye launched in 2019 a project called 'Autonomous Ready', which uses a driver support system (adas, advanced driver assistance system) to prevent collisions with pedestrians and cyclists[83]. Vehicles equipped with Mobileye technology and smart sensors (such as

www.legifrance.gouv.fr/jorf/id/JORFTEXT000043541738>).

[80] Defined as "a regulatory approach based on the principle of transparency by which companies must either comply with an established code or explain why they do not" by Forum pour l'Investissement Responsible, *Handbook no. 1, Article 173-vi: Understanding the French regulation on investor climate reporting* (2016) 37.

[81] "Both their exposure to climate-related risks and their efforts to mitigate climate change" (J. Mesonnier and B. Nguyen, *Showing off Cleaner Hands: Mandatory Climate-Related Disclosure by Financial Institutions and the Financing of Fossil Energy*, 2020, ii, retrieved 13 August 2021, <https://ssrn.com/abstract=3733781> or <http://dx.doi.org/10.2139/ssrn.3733781>).

[82] B2G data sharing practices in Barcelona have been illustrated by Manuel Valdes Lopez (General Manager of Mobility and Infrastructures) in European Commission, Event Report*, Towards green, smart and affordable mobility services in cities and communities* - 2nd B2G Data Sharing Workshop. Retrieved 13 August 2021, <https://digital-strategy.ec.europa.eu/en/library/towards-green-smart-and-affordable-mobility-services-cities-and-communities-2ndb2g-data-sharing>.

[83] The already relevant – in terms of prevention effects – outcomes can be found at https://autonomousready.org/ retrieved 13 August 2021.

buses) gather data (related to speed, surroundings, presence of pedestrian or cyclists, …) and send it to the geographic information system. In this way the government accesses data collected and generated by the private sector. Aggregated data is then used to detect risk spots and to implement safety measures and infrastructure aimed at providing better urban mobility[84]. The press release specifies that the project's aim is to extend this type of cooperation to other cities and companies as well. For this reason, Barcelona City Council has also outlined incentives for companies which might join the agreement[85].

4.3 *Florence*[86]

A third example of multilateral partnership has been developed by the city of Florence. The cooperative model of data governance used by the municipality is called Smart City Control Room (sccr)[87] and includes data collected by public transport operators (e.g., real-time data on bus positions, diversions) and by private mobility operators (e.g., bike or car sharing real-time position, battery, availability). Some peculiarities of this model should be underlined.

As opposed to the experience in Rennes described above, public transport data in Florence was initially shared due to an agreement-based model between operators and the Region of Tuscany. Then, the model was modified into the current cooperative model[88].

[84] Results are available at <https://www.barcelona.cat/infobarcelona/en/tema/mobility-andtransport/autonomous-ready-the-project-which-has-prevented-668-road-accidents-in-twomonths_887878.html>, retrieved 13 August 2021.

[85] The press release states: "El Ayuntamiento de Barcelona ha establecido una serie de incentivos para fomentar la adhesion de nuevos vehiculos a la iniciativa, entre los que destacan: facilidades de aparcamiento en superficie en las zonas destinadas a distribución urbana de mercancías de la ciudad (Zona dum); acceso a determinadas zonas en las que la movilidad rodada esta limitada al uso vecinal; ampliación del horario de carga y descarga de los vehículos de flotas que incorporen esta tecnología". (<https://autonomousready.org/salade-prensa/>, retrieved 13 August 2021).

[86] B2G data sharing practices in Florene have been illustrated by Alessandra Barbieri and Chiara Lorenzini in European Commission, Event Report, *Get started with B2G Data Sharing - 1st B2G Data Sharing Workshop*. Retrieved 13 August 2021, <https://ec.europa.eu/newsroom/dae/items/711070/en>.

[87] A detailed description can be found on the City of Florence website: <https://www.comune.fi.it/comunicati-stampa/firenze-smart-city-la-centrale-di-gestione-e-monitoraggio-trovacasa-accanto> retrieved 13 August 2021.

[88] Instead, the city of Rennes started from the data collected due to the mandatory

More specifically, regarding the bike or car sharing systems, the contracts between the city and the operators include provisions that oblige the operators to share data with the city as a precondition to provide the service. In particular, the contract between the City of Florence and RideMovi outlines a model of monitoring and reporting concerning both raw (id and type of vehicle, time and place of the ride, anonymised user id, …) and aggregated (number of vehicles, number of rides, number of users, statistics on damages or maintenance, …) data related to the mobility service[89].

This example shows how compulsory conditions requiring disclosure of information within contracts represent a different method of B2G data sharing adopted by local administrations.

4.4 *Findings*

On the basis of the analysis conducted, it is possible to assert that multilateral partnerships constitute a solid option for the future development of B2G data sharing, since, although uncommon, they seem able to obtain results on a larger scale by the cooperation of several actors, differently from bilateral partnerships.

Among several aspects, one in particular should be kept in mind: the Rennes' experience has shown that mandatory access rules imposed by law may not be sufficient to create a system which improves local decision-making processes.

These findings suggest that the direction taken by the European Commission appears to be correct. Indeed, an integrated data sharing model which relies on both voluntary agreements – stimulated by incentives to data holders – and mandatory requests based on selected prerequisites – specifically, public-interest purposes – should produce the optimal results.

In addition to that, the examples show that different methods of mandatory access rules could be implemented. Indeed, compulsory access does not necessarily occur on the basis of a law (e.g., in Rennes), but also

provision in the French energy law.

[89] Article 9 of the contract identifies the obligation of the service operator and Article 4, par. 5, f) of the contract states that object of the contract is: "the accurate collection and transmission to the Lessor of all monitoring and reporting data with the characteristics and methods indicated in the *Capitolato*" (more precisely, the monitoring is regulated by Article 12 of the document).

through contractual clauses (e.g., in Florence).

Some hints to improve the data sharing experiences also come from an analysis of technical elements: indeed, differences can be drawn between systems that collect information from sensors that most citizens use (energy consumption data) and systems that are related to certain activities only (data gained from vehicles equipped with sensors or bike-sharing data). As a consequence, it is likely that limited results will be observed within activities which rely on the second kind of data, if larger partnerships are not put into operation.

Overall, the analysis shows, on the one hand, that B2G data sharing practices could benefit from cooperating on a large scale with several economic actors involved and, on the other hand, that voluntary and mandatory access methods can actually be combined to make the circulation to be more effective.

5. *Conclusion: a European Data Governance Model to Develop B2G Data Sharing*

The analysis carried out has attempted to demonstrate how the debate on access to private data by the public sector is still at an embryonic stage, but – at the same time – that the potential output from the point of view of economic and social efficiency is such as to justify a greater attention to B2G data sharing models and practices.

Understanding the correct methods of data sharing and access to data would allow an improvement in terms of quality, as well as quantity, of the digital resources produced, collected and exchanged in digital markets[90].

[90] Moreover, since data is considered to be both the input and output of the production processes of artificial intelligence, an adequate regulatory intervention on data governance would guarantee a better understanding and development of another prominent issue in the analysis of scholars and institutions: the regulation of ai, addressed by the recent proposal of the European Commission. Since artificial intelligence's functioning and evolution are dependent on the quantity and quality of the training data used to feed their systems, the regulatory choices for both data sharing and ai tend to be inherently related. On the close connection between data and artificial intelligence, see F. Mezzanotte, *Access to Data: The Role of Consent and the Licensing Scheme*, in S. Lohsse, R. Schulze, D. Staudenmayer (ed.), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Hart/Nomos Oxford/Baden-Baden 2017) 159. Also, further, on digital markets, see V. Zeno-Zencovich, *Do "data markets" exist?"*, in *Media-Laws - Rivista di diritto dei media* 2, 2019, 22–39.

In addition, a use of shared data that is driven by the desire to pursue public interest would have a positive impact on society by enabling public authorities to perform their public tasks.

Within the business-to-government data sharing, finding the correct balance between the interests at stake requires an evaluation of the explored alternatives: a) a data sharing model exclusively grounded on a voluntary basis; b) a model that relies upon compulsory sharing between the public and private sectors; c) an intermediate option that accepts both models or that incentivizes (through compensation or reputational benefits) the practice of voluntary data-sharing, without necessarily making it compulsory.

The findings of this research show that local administrations' concrete experiences could benefit from a combination of the two models. Indeed, mandatory rules seem to be insufficient for a correct exploitation of data and could consequently benefit from forms of cooperative agreements between stakeholders.

Moreover, the case studies take a step in the direction of multilateral partnerships as an efficient method for the future development of data sharing techniques because they allow for a more complete and integrated collection of data from sensors and a more intense collaboration between the public and private sector both on a voluntary and a compulsory basis.

In order to achieve an adequate equilibrium between the illustrated solutions, it would be appropriate to carry out a cost-benefit analysis that should take into account not only the data governance legal framework, but also assess the ethical profiles that these operations might involve[91], as well as the accumulation of knowledge and, therefore, of power that data sharing implies[92]. The latter represents an aspect that, in the context

[91] P. Nemitz, *Constitutional democracy and technology in the age of artificial intelligence*, in *Philosophical Transactions of the Royal Society A* 376, 2018, 1–10, p. 10: "The works on ethic rules for technology can be precursors of the law; they can give orientation on the possible content of legal rules. But, they cannot replace the law, as they lack democratic legitimacy and the binding nature which allows enforcement with the power of government and the judiciary". The relationship between data science, law and ethics is reported in S. Benthall and J. Goldenfein, *Data Science and the Decline of Liberal Law and Ethics*, 2020, available at ssrn: <https://ssrn.com/abstract=3632577 or http://dx.doi.org/10.2139/ssrn.3632577>.

[92] Richter, *The law and policy of government access to private sector data ('B2G data sharing')*, cit., p. 532; M. J. Slaughter and D. H. McCormick, *Data Is Power. Washington Needs to Craft New Rules for the Digital Age*. 2021. Foreign Affairs, May/June. Retrieved 29 April 2021, <https://www.foreignaffairs.com/articles/united-states/2021-04-16/data-power-new-rules-digital-age>.

of relations between the public and private sectors, cannot be neglected: from this point of view, it appears clear that "Europe is striving to find a middle way between the two opposite models of 'state-led innovation' (China) and a 'purely decentralized market system' (USA)"[93].

[93] Resta, *Data and Territory. The impact of the "local" in the regulation of digital technologies and algorithmic decision-making*, cit., p. 17–18, in which, again, the two major issues identified are the legal regime of non-personal data and government access to private sector data (B2G); cf. also Streinz, *The Evolution of European Data Law*, cit., p. 47. More generally, about the relationship between Europe and the China-USA regulatory dichotomy, see also M. S. Erie, T. Streinz, *The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance*, in *N.Y.U. J. Int'l L. / Pol.*, vol. 54, 2021, 1-92.

Autori/Contributors

Paolo Cavaliere, *Lecturer in Digital Media and IT Law*, *University of Edinburgh Law School*.

Licia Cianci, *Academic Fellow*, *Bocconi University*.

Edoardo Chiti, *Professore ordinario di Diritto amministrativo*, *Università della Tuscia e Sant'Anna di Pisa*.

Fabiana Di Porto, *Professor of Law and Tech at the University of Salento and Contract Professor of Innovation Law and Regulation*, *LUISS Guido Carli (Roma)*.

Maria Samantha Esposito, *Assistant Professor of Private Law*, *Turin Polytechnic*.

Giulia Ferrari, *Ph.D. in Business e Social Law*, *Bocconi University*.

Daniel Foà, *Dottore di ricerca in Diritto e Impresa*, *Università LUISS Guido Carli (Roma)*.

Tatjana Grote, *LLM Candidate, London School of Economics and Political Science*.

Riccardo Invernizzi, *Junior Analyst at DAAT consulting*.

Alessandro Mantelero, *Associate Professor of Private Law and Law & Technology*, *Turin Polytechnic*.

Barbara Marchetti, *Professoressa ordinaria di Diritto amministrativo*, *Università degli Studi di Trento*.

Mariateresa Maggiolino, *Professore associato di diritto commerciale*, *Università Commerciale Luigi Bocconi*.

Nicoletta Rangone, *Professoressa ordinaria di diritto amministrativo*, *Università LUMSA (Roma)*.

Giorgio Resta, *Full Professor of Comparative Law*, *Roma Tre University*.

Graziella Romeo, *Associate Professor of Comparative Constitutional Law*, *Bocconi University*.

Annalisa Signorelli, *Assegnista di ricerca*, *Università degli studi Roma Tre*.

Vanessa Villanueva Collao, *Research Fellow*, *Roma Tre University and JSD candidate, University of Illinois*.

Gabriele Volpi, *Manager, DAAT consulting*.

Andrea Vigorito, *Assegnista di ricerca*, *Università degli studi Roma Tre*.

Davide Zecca, *Academic Fellow*, *Bocconi University*.

Vincenzo Zeno-Zencovich, *Full Professor of Comparative Law*, *Roma Tre University*.

Marialuisa Zuppetta†, *Assistant Professor of Public Law*, *Università degli Studi del Salento*.

ROMA TRE
UNIVERSITÀ DEGLI STUDI

These two volumes collect twenty five articles and papers published within the "Governance of/through Big Data" research project financed by the Italian Ministry of Universities. The research project, which was promoted by Roma Tre University, as project lead, and saw the participation of professors and reseachers from Bocconi University in Milan; LUMSA University in Rome; Salento University in Lecce and Turin Polytechnic, covers multiple issues which are here presented in five sections: Algorithms and artificial intelligence; Antitrust, artificial intelligence and data; Big Data; Data governance; Data protection and privacy.

Giorgio Resta and **Vincenzo Zeno-Zencovich** are full professors of comparative law in the Roma Tre University.

Roma TrE-Press
2023