

Guido D'Ippolito

**IL PRINCIPIO DI LIMITAZIONE
DELLA FINALITÀ DEL
TRATTAMENTO TRA *DATA
PROTECTION* E ANTITRUST.
IL CASO DELL'USO
SECONDARIO DI BIG DATA**

Estratto



GIUFFRÈ FRANCIS LEFEBVRE

GUIDO D'IPPOLITO

IL PRINCIPIO DI LIMITAZIONE DELLA FINALITÀ DEL TRATTAMENTO TRA *DATA PROTECTION* E ANTITRUST. IL CASO DELL'USO SECONDARIO DI BIG DATA

SOMMARIO: 1. Introduzione: la tendenza all'uso secondario di big data. — 1.1. La gestione dei dati tra antitrust e *data protection*. — 2. Il principio di limitazione della finalità del trattamento. — 2.1. Compatibilità del trattamento ulteriore. — 3. Uso secondario e trasparenza. — 4. Uso secondario e base giuridica dell'ulteriore trattamento. — 5. Il caso Facebook/WhatsApp. — 6. Rimedi *ex ante* avverso trattamenti abusivi dei dati personali: gli artt. 20 e 25 GDPR. — 7. Il diritto di opposizione. — 8. Conclusioni.

1. INTRODUZIONE: LA TENDENZA ALL'USO SECONDARIO DI BIG DATA.

Il recente sviluppo economico, dominato sempre più dal ruolo delle piattaforme digitali quali nuovi modelli di “*two-sided market*”¹, vede nella raccolta massiva e successiva rielaborazione di dati uno dei suoi elementi più vitali tanto da poter parlare ormai di “economia dei dati”² e di “*knowledge-based economy*”³. Tanto più questo è vero con riferimento ai i cc.dd. soggetti “*Over the*

¹ Con riferimento alle piattaforme digitali e big data si vedano J-S. BERCÉ, S. GRUMBACH, V. ZENO-ZENCOVICH, *The 'Data-sphere', Data Flows beyond Control, and the Challenges for Law and Governance*, in *European Journal of Comparative Law and Governance*, 5, 2018, p. 144-17; G. RESTA, *Digital platforms and the law: contested issues*, in *MediaLaws Rivista di diritto dei media*, 2018, fasc. 1, p. 231-248; M.R. ROSSI, *Il ruolo delle piattaforme nell'economia dei big data*, in V. FALCE, G. GHIDINI, G. OLIVIERI (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2017, p. 75-92; G. COLANGELO, *Big data, piattaforme digitali e antitrust*, in *Mercato concorrenza regole*, 2016, fasc. 3, p. 425-460.

² Per approfondire lo studio della c.d. *digital economy* si veda ITMedia Consulting con il contributo scientifico dell'Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, Roma, Gennaio 2018, reperibile al seguente link: www.itmedia-consulting.com/it/highlights/1187-l-economia-dei-dati-tendenze-di-mercato-e-prospettive-di-policy-lo-studio-fondamentale-sui-big-data-2.html; Si veda anche V. BAGNOLI, *The big data relevant market*, in *Concorrenza e mercato*, fasc. 1, 1 gennaio 2016, p. 79 ss., per il quale il settore dell'economia digitale è caratterizzato da forte crescita, apparizione di nuovi servizi, concentrazione del mercato con pochi attori in posizione dominante e uno squi-

top” per i quali informazioni e dati (personali e non) ⁴ diventano *asset* importanti nei rispettivi *business model*.

La raccolta massiva e il successivo utilizzo di dati diventa quindi l'elemento abilitante di nuove attività di business. Sebbene la raccolta di grandi quantità di dati (*big data* ⁵) di per sé solo non sia sufficiente, essendo necessario investire nell'ottenimento e nello sviluppo di appositi algoritmi che trasformino i dati grezzi (*input*) in informazioni utilizzabili (*output*) e che quindi estraggano (e attribuiscono) valore dai dati (creando altri dati), questi possono comunque essere considerati una risorsa indispensa-

librio crescente tra grandi aziende da un lato e piccole e medie imprese e consumatori dall'altro.

³ L'espressione è usata da Pitruzzella (G. PITRUZZELLA, *Big Data, Competition and Privacy: A look from the antitrust perspective*, in *Concorrenza e Mercato*, fasc. 1, 1 gennaio 2016, p. 16) e sembra riprendere e applicare al mercato l'espressione di “*società della conoscenza*” usata da Rodotà con riferimento alle moderne democrazie e società in generale (S. RODOTÀ, *Il diritto di avere diritti*, Bari, 2013, p. 135).

⁴ Nel prendere atto della sempre più difficile distinzione tra ciò che è tecnicamente un dato personale e ciò che non lo è, dovuto alla difficoltà di qualificare in modo certo un dato come appartenente stabilmente a una categoria piuttosto che all'altra, nel corso di questa trattazione, laddove possibile, si farà esplicito riferimento al “dato personale” o non personale. Negli altri casi, pur consapevoli dell'inevitabile imprecisione, si utilizzerà la formula generica “dato” per intendere complessivamente sia l'una che l'altra categoria. Con riferimento ai dati non personali, si tenga conto che, da una parte essi sono esclusi dall'ambito di applicazione del Regolamento UE 2016/679, dall'altro sono oggetto di specifica normativa (cfr. Proposal for a Regulation on a framework for the free flow of non-personal data in the European Union (COM(2017)495) http://europa.eu/rapid/press-release_STATEMENT-18-6001_it.htm)

⁵ Col termine “big data” si fa riferimento a « ingenti quantità di dati disponibili all'interno del nuovo ecosistema digitale, prodotti ad alta velocità e provenienti da una moltitudine di fonti, la cui gestione e analisi richiedono nuovi e più potenti processori e algoritmi ». Così da ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 94. Con riferimento alla

gestione dei big data in relazione ai temi della presente trattazione, si vedano F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018; V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *MediaLaus Rivista di diritto dei media*, 2/2018 e *Come il mondo dei dati cambia taluni riferimenti tradizionali del giurista*, in F. DI CIOMMO, O. TROIANO (a cura di), *Scritti in onore di Roberto Pardolesi*, Piacenza, 2018, p. 107-115; L. CALIFANO, *Brevi riflessioni su privacy e costituzionalismo al tempo dei big data*, in *Federalismi.it*, fasc. 9, 2017; FALCE, G. GHIDINI, G. OLIVIERI (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2017; G. PITRUZZELLA, *Big data and antitrust enforcement*, in *Italian Antitrust Review*, Vol 4, No 1, 2017, p. 77-86; M. OREFICE, *I “big data”. Regole e concorrenza (Big Data. Rules and Competition)*, in *Politica del diritto*, fasc. 4, 2016, p. 697-743. In tema di big data si registra l'avvio, in data 30 maggio 2017, dell'indagine conoscitiva sui Big Data da parte de l'Autorità Garante della Concorrenza e del Mercato, l'Autorità per le Garanzie nelle Comunicazioni e il Garante per la Protezione dei Dati Personali. Tale indagine ha finora prodotto, in data 8 giugno 2018: da parte dell'AGCOM, un “*Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*”, reperibile al link: <https://www.agcom.it/documents/10179/10875949/Studio-Ricerca+08-06-2018/c72b5230-354d-444f-9e3f-5467ca450714?version=1.0>; e da parte dell'AGCM, i primi risultati della “*Analisi della propensione degli utenti on line a consentire l'uso dei propri dati a fronte dell'erogazione di servizi*”, reperibile al link: www.agcm.it/stampa/comunicati/9334-ic53-primi-risultati-dell-indagine-conoscitiva-sui-big-data-congiunta-con-agcom-e-garante-privacy.html

bile⁶. In quest'ottica, e mettendo da parte in tale trattazione le questioni relative all'algoritmo, l'utilizzo e il riutilizzo dei big data produce effetti rilevanti sia in ottica antitrust che in ottica *data protection*.

Nello specifico, delimitando meglio l'area d'indagine con riferimento alla normativa in materia di protezione dei dati personali seppur con una imprescindibile prospettiva economica e di regolazione dei mercati, si cercherà di affrontare la tendenza dalle più grandi piattaforme digitali di entrare in settori terzi rispetto a quelli propri⁷. Dal punto di vista della gestione dei dati sottesa a tale tendenza, si può inquadrare la questione nella fattispecie definita di "uso secondario⁸ o alternativo di big data".

I fornitori di servizi digitali già da tempo hanno iniziato a raccogliere dati personali su vasta scala per svolgere la loro attività in un certo mercato. Tuttavia, una volta raggiunta una posizione dominante nel mercato di riferimento, questi stessi fornitori si sono rivolti ad altri mercati. In tal caso, i fornitori hanno iniziato ad elaborare i dati raccolti anche per fornire altri servizi in altrettanti mercati oppure ad acquistare data set da altre imprese per rielaborarli con quelli già in proprio possesso e fornire ulteriori servizi⁹.

Si pensi, da ultimo, al recente episodio che vede Facebook al centro di polemiche per presunti usi illeciti di dati personali. Nello specifico, Facebook avrebbe richiesto ad alcuni gruppi bancari americani i dati dei propri clienti nel tentativo di offrire a quest'ultimi, quali utenti della piattaforma social, nuovi servizi di carattere finanziario¹⁰. Ma si pensi soprattutto alle intenzioni di

⁶ ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 101 ss.

⁷ La tendenza dell'ingresso in Italia in ciascuno dei mercati regolati (comunicazioni, energia, banche, mercati finanziari, assicurazioni, trasporti) di un operatore nuovo specializzato nella raccolta e gestione dei dati è esaminata dall'undicesimo rapporto annuale "Consumerism 2018", elaborato dal Consumer's Forum e l'Università degli studi Roma Tre, dal titolo "Il cittadino nell'era dell'algoritmo", novembre 2018, disponibile al link: www.consumersforum.it/ricerche.html Il fenomeno è esaminato anche da ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 103 ss.

⁸ A.M. CARDANI, *Relazione annuale 2018 sull'attività svolta e sui programmi di lavoro dell'Autorità per le Garanzie nelle Comunicazioni. Presentazione del Presidente dell'Autorità*, 11 luglio 2018, p. 22, consultabile al seguente link: www.agcom.it/

documents/10179/11258925/Discurso+del+Presidente/f5adf6bc-b4ce-40ac-8f51-3cf61e9f83ee.

⁹ ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 108 e ss.; European Data Protection Supervisor (EDPS), *Preliminary Opinion of the European Data Protection Supervisor. Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, March 2014, §58, consultabile al link: https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-and-competitiveness-age-big-data_en.

¹⁰ B. SIMONETTA, *Facebook chiede alle banche di condividere i dati dei loro clienti*, in *Il Sole 24 Ore*, 6 agosto 2018, www.ilsole24ore.com/art/tecnologie/2018-08-06/facebook-ha-chiesto-banche-condividere-dati-loro-clienti-181757.shtml?uuid=AEfbowXF.

piattaforme come Amazon che, sfruttando anche la nuova disciplina sui sistemi di pagamento, mirano ad entrare nel settore bancario¹¹. Tutto ciò genera un'ulteriore accelerazione della corsa al dato, sempre più risorsa fondamentale di nuove attività economiche, come testimoniato dalla scoperta di un accordo tra Google e Mastercard in base al quale il secondo cedeva al primo i dati dello "shopping offline" dei suoi clienti per permettere a Google di meglio analizzare gli effetti delle sue inserzioni pubblicitarie anche là dove non potrebbe arrivare, ossia agli acquisti nel mondo fisico¹².

Come si vedrà, la fattispecie dell'uso secondario di big data ha quindi riflessi simultaneamente sia in materia di protezione dei dati personali, sia in ambito di tutela della concorrenza ma anche del consumatore/utente¹³, dove si può assistere per esempio a pratiche commerciali scorrette o clausole vessatorie¹⁴. Ed infatti se la scorretta gestione dei dati personali può portare a integrare comportamenti anti-competitivi o ipotesi di abuso di posizione dominante¹⁵, allo stesso tempo potrebbe porsi in contrasto con i principi relativi al trattamento lecito e corretto dei dati personali, andando così a ledere gli interessi di quel soggetto che contempo-

¹¹ In seguito alla Direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD2), pienamente operativa dal 13 gennaio 2018, le grandi piattaforme digitali in qualità di "Third Party Providers" (TPP) potranno direttamente accedere ai dati sui conti correnti bancari degli utenti. Le banche saranno infatti tenute ad aprire le loro *Application Programming Interfaces* (APIs) per permettere a terze parti di accedere ai dati dei clienti e offrire innovativi servizi in concorrenza con le stesse banche. Previo consenso degli utenti/interessati gli operatori OTT, a partire dai cc.dd. GAFAM (Google, Amazon, Facebook, Apple, Microsoft), potranno infatti offrire servizi che, per esempio, permetteranno di inviare denaro ad un amico semplicemente digitando la dicitura "+10 euro" nella corrispondente chat dell'app di messaggistica. Sul tema si veda V. FLOCCARI, A. INGENITO, L'ingresso degli *Over the Top* nel mercato dei servizi di pagamento, in rapporto Consumerism 2018 su "Il cittadino nell'era dell'algoritmo" realizzato da Consumers' Forum e Università Roma Tre, p. 67-81.

¹² Il Sole 24 Ore, *Google e Mastercard, patto segreto per tracciare gli acquisti offline*, 31 agosto 2018, disponibile al link: www.ilsole24ore.com/art/tecnologie/2018-08-31/google-e-mastercard-patto-segreto-tracciare-acquisti-offline--103746.shtml?uuid=AEacQqF&refresh_ce=1.

¹³ G. PITRUZZELLA, *Big data and anti-trust enforcement*, in *Italian Antitrust Review*, Vol 4, No 1 (2017), p. 77-86; ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 264 ss.

¹⁴ V. BAGNOLI, *The big data relevant market*, in *Concorrenza e mercato*, fasc. 1, 1 gennaio 2016, p. 74 e ss.; G. RESTA, *Digital platforms and the law*, cit., p. 237 ss. Si vedano anche i provvedimenti dell'AGCM: PS10601 e CV154 dell'11/05/2017 - WhatsApp ha indotto gli utenti a condividere i loro dati con Facebook: www.agcm.it/media/dettaglio?id=61dde0b6-d8aa-4a34-b9c8-aeb9a39ee71e. Nonché PS11112 del 7/12/2018 - Uso dei dati degli utenti a fini commerciali: sanzioni per 10 milioni di euro a Facebook: www.agcm.it/media/comunicati-stampa/2018/12/Uso-dei-dati-degli-utenti-a-fini-commerciali-sanzioni-per-10-milioni-di-euro-a-Facebook.

¹⁵ I comportamenti anticompetitivi che possono derivare dalla gestione dei big data hanno rilievo nell'ambito degli abusi di posizione dominante, delle operazioni di concentrazione e acquisizione, condotte escludenti derivanti dal rifiuto di accesso o accesso discriminatorio ai dati, da contratti di esclusiva, vendite vincolate (c.d. *tying*) o utilizzo incrociato di data set, ancora l'utilizzo di dati per realizzare attività di *price discrimination*, ecc. Con riferimento agli abusi di posizione dominante e pratiche col-

ranicamente riveste il ruolo di consumatore, utente, interessato del trattamento.

1.1. *La gestione dei dati tra antitrust e data protection.*

Il ruolo che i big data svolgono nel mercato on line ha posto la domanda se i dati possano essere considerati un elemento essenziale e considerati quindi un “*essential facility*”¹⁶. Tradizionalmente l'impatto della gestione dei big data sulla struttura del mercato è esaminato secondo due prospettive antitetiche. Secondo una prima visione i big data sarebbero un asset fondamentale, controllato da imprese in posizione dominante, che impedisce ai concorrenti di entrare nel relativo mercato¹⁷. Diversamente, per una seconda visione i dati sarebbero beni liberamente accessibili da parte di chiunque, da una varietà di fonti, spostando l'attenzione sulle capacità e le possibilità che le imprese hanno di gestire i dati e offrire servizi innovativi e di migliore qualità ai consumatori¹⁸. In entrambi i casi, la gestione dei dati tocca sia la materia della protezione dei dati personali che quella della tutela della

lusive si veda G. MUSCOLO, *Big data e concorrenza. Quale rapporto?*, p. 178 e ss., in V. FALCE, G. GHIDINI, G. OLIVIERI (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2017; A. EZRACHI, M.E. STUCKE, *Artificial Intelligence & Collusion: When Computers Inhibit Competition*, University of Illinois Law Review, 2017, Oxford Legal Studies Research Paper No. 18/2015, University of Tennessee Legal Studies Research Paper No. 267, disponibile al link: <https://ssrn.com/abstract=2591874> o <http://dx.doi.org/10.2139/ssrn.2591874>. Con riferimento alle possibili discriminazioni prodotte dalla personalizzazione dei prezzi tramite algoritmi si vedano: M. MAGGIOLINO, *Big data e prezzi personalizzati*, in *Concorrenza e mercato*, fasc. 1, 1 gennaio 2016, p. 95-138; ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 247 ss. Il tema è stato analizzato anche dalla Competition and Markets Authority nel paper “*Pricing algorithms. Economic working paper on the use of algorithms to facilitate collusion and personalised pricing*”, 8 October 2018, CMA94, disponibile al link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746353/Algorithms_econ_report.pdf.

¹⁶ Sul punto, un invito alla cautela nell'attribuzione quasi-automatica ai big data della targhetta di risorsa essenziale è formulato da A. PEZZOLI, *Big data e antitrust: un'occasione per tornare ad occuparci di*

struttura?, p. 252 e ss., in V. FALCE, G. GHIDINI, G. OLIVIERI (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2017; si veda anche G. PITRUZZELLA, *Big data and antitrust enforcement*, cit., p. 79.

¹⁷ Con riferimento alla domanda, più volte posta in dottrina, relative al se e al quanto il possesso di data set da parte di un operatore possa attribuire un vantaggio competitivo non replicabile dalle imprese concorrenti si vedano in senso favorevole: A. EZRACHI, M.E. STUCKE, *Virtual Competition. The promise and perils of the algorithm-driven economy*, in *Harvard University Press*, 2016; M.E. STUCKE, A.P. GRÜNES, *Big Data and competition policy*, in *Oxford University Press*, 2016; G. PITRUZZELLA, *Big Data, competition and privacy: a look from the antitrust perspective*, in *Concorrenza e mercato*, 2016, p. 15 ss.; Id., *Big Data and antitrust enforcement*, in *Italian Antitrust Review*, 2017, p. 77 ss.; V. BAGNOLI, *The big data relevant market*, in *Concorrenza e mercato*, fasc. 1, 1 gennaio 2016, p. 73-94.

¹⁸ In tal senso si vedano: D.D. SOKOL, R. COMERFORD, *Does antitrust have a role to play in regulating Big Data?*, in *Cambridge handbook of Antitrust, Intellectual Property and High Tech*, Cambridge University Press, 2016; A. LAMBRICHT, C. TUCKER, *Can Big Data protect a firm from competition?*, Working paper, 18 dicembre 2015, https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2705530; D.S. TUCKER, H. WELFORD, *Big mistakes regarding Big Data*,

concorrenza, ma, come si vedrà nel prosieguo, anche dei consumatori, con la conseguente necessità di affrontare la tematica non per compartimenti stagni ma in modo correlato e interrelato tra le discipline coinvolte¹⁹. Ciò porta immediatamente a chiedersi se e quanto una data situazione sia meglio risolvibile alla luce della normativa *data protection* o di *competition* o se ognuna può diventare elemento di valutazione dell'altra²⁰.

Scopo di tale trattazione è quindi verificare se il ricorso alla normativa in materia di protezione dei dati personali può essere utile per regolare il riutilizzo dei dati servendo come ulteriore elemento di valutazione per altre aree normative. In particolare, si cercherà di analizzare come alcuni istituti tipici della protezione dei dati personali, a partire dal principio di limitazione della finalità del trattamento, possano innanzitutto aiutare a individuare le regole che rendano lecito l'utilizzo di dati personali nel passaggio da una finalità (e quindi trattamento) all'altra; secondariamente se tali norme possano avere rilievo nell'ambito di attività proprie del diritto della concorrenza ed essere d'ausilio nelle valutazioni in tema di abusi di posizione dominante, concentrazioni o alterazione della concorrenza. Ed infatti, le questioni relative alla privacy e alla protezione del dato, in quanto asset economico ed ulteriore elemento di concorrenza tra le imprese, è rilevante per la normativa sulla concorrenza sia con riferimento al valore economico del dato sia perché potrebbe contribuire come ulteriore elemento sintomatico nelle tipiche valutazioni antitrust²¹.

Dunque, tramite una convergenza della disciplina *data protection* con quella di *competition* si cercherà di analizzare se e come evitare o rimediare a fenomeni lesivi tanto della riservatezza e corretta gestione dei dati personali quanto della concorrenza.

Ciò non al fine di vietare o ostacolare lo sviluppo e le tendenze degli operatori del mercato bensì con l'intento di individuare delle regole, disegnare un perimetro di liceità, rendere chiara e il più

in *Antitrust Source*, dicembre 2014; A.V. LERNER, *The role of "Big Data" in online platform competition*, Working paper, 2014, https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2482780.

¹⁹ Per un'analisi economica delle questioni relative alla protezione dei dati personali nel contesto digitale, in ottica convergente tra più normative, si veda W. KERBER, *Digital markets, data, and privacy: competition law, consumer law and data protection*, in V. FALCE, G. GHIDINI, G. OLIVIERI (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2017, p. 1-20, secondo il quale (p. 2): « in order to address properly the concerns about pri-

vacy in the digital economy, it is not sufficient to look for policy solution in one field of law alone, e.g. competition law or data protection, but that an integrated approach from various regulatory perspectives that can be deemed relevant to privacy concerns ».

²⁰ G. PITRUZZELLA, *Big Data, Competition and Privacy: A look from the antitrust perspective*, in *Concorrenza e Mercato*, fasc. 1, 1 gennaio 2016, p. 24 ss.

²¹ Per verificare in quali casi e come i dati personali assumano rilievo economico commerciale per le imprese si veda: W. KERBER, *Digital markets, data, and privacy: competition law, consumer law and data protection*, cit., p. 4 ss.

certa possibile la normativa che delimita il campo all'interno del quale le imprese possano muoversi nel rispetto dei diritti dei soggetti coinvolti, andando ad inibire e sanzionare solo quei comportamenti integranti fenomeni abusivi. Più nello specifico, a partire dal principio di limitazione delle finalità, si andranno ad individuare e analizzare quegli istituti di *data protection* che non solo permettono una corretta gestione dei dati personali ma, all'occorrenza, potrebbero anche essere d'ausilio nell'ambito di valutazioni antitrust, come sarà più dettagliatamente illustrato nel prosieguo.

Questo anche alla luce del fatto che la disciplina in tema di *data protection*, specie dopo il Regolamento generale sulla protezione dei dati personali (UE) 2016/679 ("*General Data Protection Regulation*" o "GDPR"), non ha come obiettivo quello di vietare l'uso di dati personali ma di bilanciare due interessi ugualmente meritevoli di tutela: la protezione dei diritti e delle libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, e la tutela del mercato, la libera circolazione di tali dati e quindi l'incentivo alle più innovative attività di impresa²². Tutela dei diritti fondamentali ed esigenze del mercato non dovrebbero infatti essere considerati principi contrapposti²³.

L'indagine sarà quindi condotta sulla base di alcuni istituti in materia di *data protection*, senza però potersi esimere dal tener conto della normativa sulla concorrenza laddove anche questa ha come scopo garantire la correttezza e il rispetto dei diritti all'interno dei mercati al fine di permetterne lo sviluppo generale²⁴. Da più parti è infatti sottolineata la necessità oltre che l'utilità di una convergenza tra queste due discipline in modo da meglio affrontare le nuove sfide poste dall'economia digitale²⁵.

²² Cfr. art. 1 Regolamento UE/2016/679. Si vedano anche, in particolare, i considerando n. 4: « Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemplato con altri diritti fondamentali, in ossequio al principio di proporzionalità [...] » e 6: « [...] La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione ».

²³ G. PITRUZZELLA, *Big Data, Competition and Privacy: A look from the antitrust perspective*, in *Concorrenza e Mercato*, fasc. 1, 1 gennaio 2016, p. 15-28.

²⁴ Cfr. M. LIBERTINI, *La concorrenza degli antichi e la concorrenza dei moderni*, in C. RABITTI BEDOGNI, P. BARUCCI (a cura

di), *20 anni di antitrust. L'evoluzione dell'Autorità Garante della Concorrenza e del Mercato*, Torino, 2010, p. 109, per il quale: « la tutela della concorrenza [deve intendersi] non più come tutela di una certa struttura di mercato ma come disciplina volta a realizzare l'obiettivo del massimo benessere del consumatore ». Si vedano anche: ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 187 e ss che rinviene nella tutela del corretto funzionamento del mercato in relazione al variare del benessere dei consumatori il bene giuridico protetto dalla normativa antitrust; V. BAGNOLI, *The big data relevant market*, in *Concorrenza e mercato*, fasc. 1, 1 gennaio 2016, p. 73 ss.

²⁵ G. RESTA, *Digital platforms and the law*, cit., p. 245; EDPS, *Privacy and com-*

In tal senso si potrebbe dire che entrambe le normative qui coinvolte hanno in comune l'obiettivo di permettere un utilizzo lecito dei dati, personali e non, per creare quel clima di fiducia indispensabile per lo sviluppo dell'economia digitale ²⁶. Tanto le norme in materia di competizione (ma, come già detto, anche quelle a tutela del consumatore ²⁷) quanto le norme sulla protezione dei dati personali possono quindi essere usate come strumento per promuovere l'efficienza nei mercati digitali e incoraggiare l'innovazione ²⁸.

All'esito della trattazione, si cercherà infine di individuare alcuni rimedi e strumenti che, in relazione alla fattispecie di uso secondario di big data, sono diretti a inibire e sanzionare fenomeni abusivi rilevanti sia per il settore della privacy che della *competition*. A tal fine si cercherà di far emergere la valenza antitrust di alcuni istituti propri del GDPR. Gli istituti coinvolti saranno quindi innanzitutto il principio di limitazione delle finalità del trattamento dei dati personali e, in conseguenza di questo, le basi di liceità del trattamento.

Tra i rimedi ad abusi nell'utilizzo dei dati suscettibili di integrare una distorsione del mercato si possono annoverare soprattutto gli istituti della c.d. *data protection by design* e *by default* e il nuovo diritto alla portabilità dei dati. Questi istituti suscitano particolare interesse perché si pongono come rimedi *ex ante*, inibitori di comportamenti scorretti e che si inseriscono nella tematica dei *privacy-enhancing services* ²⁹.

Con riferimento ai rimedi *ex post*, si può ricorrere al diritto di opposizione e, in generale, ai tradizionali strumenti di tutela in mano alle autorità amministrative indipendenti, all'autorità giudiziaria e agli altri organi e soggetti coinvolti.

petitiveness in the age of big data, cit., p. 3. G. PITRUZZELLA, *Big Data, Competition and Privacy*, cit., p. 26 e ss.; W. KERBER, *Digital markets, data, and privacy: competition law, consumer law and data protection*, cit., p. 1-20; G. MUSCOLO, *Big data e concorrenza. Quale rapporto?*, p. 185 ss.

²⁶ EDPS, *Privacy and competitiveness in the age of big data*, cit., §2: « EU principles and rules on data protection, competition and consumer protection have been designed to promote a thriving internal market and to protect the individual. Greater convergence in the application of these policies could help meet the challenges posed by the big data economy. However, to date, policies have tended to develop in parallel with little interaction on subjects of common concern ».

²⁷ W. KERBER, *Digital markets, data, and privacy: competition law, consumer*

law and data protection, cit., p. 12: « Since European consumer law has the objectives of protecting the health, safety, and economic interests of the consumers, it also protects the privacy of consumer as part of their economic interests and safety but also as their fundamental right ».

²⁸ EDPS, *Privacy and competitiveness in the age of big data*, cit., § 33.

²⁹ La Commissione Europea, nella COM (2007) 228: « *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)* », definisce *Privacy-enhancing technologies* come « coherent system of information and communication technology measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data without losing the functionality of the information system ».

2. IL PRINCIPIO DI LIMITAZIONE DELLA FINALITÀ DEL TRATTAMENTO.

In astratto, l'ingresso di un nuovo operatore in un mercato non dovrebbe sollevare criticità sotto il profilo della concorrenza. Al contrario è visto con favore nella misura in cui ciò potrebbe smuovere equilibri consolidati e andare a vantaggio della concorrenza generale. Ciò vale anche se ad entrare in un nuovo mercato sono soggetti “*Over the top*” e giganti del digitale. Tuttavia alcuni profili di criticità potrebbero aversi se, per esempio, questi ultimi avessero accesso a dati a cui i concorrenti non possono accedere³⁰. Se questi sono dati personali, dalla disciplina sulla concorrenza si passa a quella sulla tutela dei dati personali con la conseguenza che il rispetto delle norme sul corretto trattamento può avere riflessi di carattere concorrenziale e aiutare a evitare fenomeni distorsivi della concorrenza.

Ci si sposta così alla disciplina *data protection* per la quale il passaggio dal mercato in cui tradizionalmente opera una certa impresa ad un nuovo mercato oppure la prestazione di un nuovo servizio è da considerarsi legittimo in presenza di alcune condizioni. Per esempio quando l'impresa X, operante nel mercato X, nel momento in cui decide di entrare anche nel mercato Y per svolgere un nuovo servizio Y, imposta da zero una nuova attività di trattamento. Questo vuol dire realizzare un nuovo *data base* nel quale raccogliere i dati necessari per la nuova attività.

In questo caso non si pongono particolari problematiche rilevanti né per la privacy né per la concorrenza. Accumulare un'enorme quantità di dati in un nuovo mercato non è un'attività di per sé illecita né con riferimento alle norme sulla protezione dei dati personali né con riferimento a quelle sulla concorrenza. In tal caso e con riferimento alla gestione dei dati, il punto di partenza, ossia la creazione di un proprio *data base*, è lo stesso per ogni operatore.

Diversamente, qualche attenzione in più sarà necessaria nel momento in cui l'impresa X decida di offrire il nuovo servizio Y (magari anche in un altro mercato Y) usando però i dati precedentemente raccolti e trattati per il servizio X. Che questo possa essere un comportamento particolarmente profittevole per grandi multinazionali del digitale, in particolare i cc.dd. soggetti “GA-FAM”³¹, è di facile intuizione laddove la disponibilità di enormi

³⁰ G. PITRUZZELLA, *Big data and anti-trust enforcement*, cit., p. 79. Cfr. ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 214 e ss e 235 ss.

³¹ Il termine GAFA è l'acronimo di Google, Apple, Facebook e Amazon e indica, cumulativamente, le più grandi piat-

taforme digitali ossia le società tecnologiche più di successo a livello mondiale: Alphabet Inc. (Google), Apple Inc., Facebook e Amazon. Successivamente si è aggiunta un'ultima lettera, la M, con riferimento a Microsoft. Cfr. P. SIMON, *The Age of the Platform: How Amazon, Apple, Facebook, and Google Have Redefined Business*, Motion

quantità di dati e, soprattutto, la possibilità di incrociarli con i nuovi dati derivanti dall'ulteriore attività potrebbe comportare un vantaggio competitivo distorsivo delle dinamiche del nuovo mercato³². Tale comportamento andrebbe infatti ad aggravare le due principali “*theories of harm*” relative alla gestione dei big data³³, ossia sfruttare il potenziale di preclusione che il controllo dei dati può avere sulla fornitura di beni o servizi nei mercati a valle e l'utilizzo abusivo dei big data, portando al risultato per cui “*winner takes all*”³⁴.

Simili conseguenze possono essere evitate applicando il principio di limitazione della finalità del trattamento, uno dei capisaldi del corretto trattamento dei dati personali³⁵.

A partire dall'art. 5 della Convenzione 108/1981³⁶, secondo il quale « I dati a carattere personale oggetto di elaborazione automatica devono essere registrati per fini determinati e legittimi e non devono essere utilizzati in modo incompatibile con tali fini », fino all'art. 8 della Carta dei diritti fondamentali dell'Unione Europea. Il secondo comma di tale articolo infatti prevede che i

Publishing, 2011, e S. GALLOWAY, *The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google*, Portfolio, 2017 (ed. italiana di Hoepli, 2018).

³² D. QUAGLIONE - C. POZZI, *Economia dei big data: Lineamenti del dibattito in corso e alcune riflessioni di policy*, in *L'industria*, XXXIX, n. 1, gennaio-marzo 2018, p. 4; M. CAPPAL, *Social economy, gestione dei dati e tutela della concorrenza*, in *Consumerism 2017. Decimo Rapporto annuale: Dalla sharing alla social, alla data economy. Big data, fake news, privacy e pubblicità*, p. 40-48; V. BAGNOLI, *The big data relevant market*, cit., p. 73 e ss.; M. GAMBARO, *Big data, mercato e mercati rilevanti*, p. 193-209, in V. FALCE, G. GHIDINI, G. OLIVIERI (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2017.

³³ Per una ricognizione della più importanti *theories of harm* prospettate con riferimento alla gestione dei big data si veda G. COLANGELO, M. MAGGIOLINO, *Big data, Protection and Antitrust in the wake of the Bundeskartellamt case against Facebook*, in *Italian Antitrust Review*, n. 1, 2017, p. 106 ss. Si veda anche ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 258 e ss, dove si ritiene che, con riferimento alla commercializzazione di prodotti e servizi “*privacy-friendly*” e di tecnologie “*privacy-enhancing*”, per permettere un intervento antitrust volto a sanzionare eventuali strategie capaci di ridurre la qualità e quantità di questi beni e servizi non vi

sarebbe necessità di sviluppare alcuna particolare teoria del danno perché quei comportamenti sarebbero semplicemente riduttivi del *consumer welfare* di coloro che tali beni intendono acquistare.

³⁴ G. PITRUZZELLA, *Big Data, Competition and Privacy*, cit., p. 17 e ss.; G. MUSCOLO, *Big data e concorrenza. Quale rapporto?*, p. 175, in V. FALCE, G. GHIDINI, G. OLIVIERI (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2017.

³⁵ European Union Agency for Fundamental Rights - Council of Europe - European Court of Human Rights - European Data Protection Supervisor, *Handbook on European data protection law*, 2018 edition, p. 122; Si vedano anche: C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, p. 110; Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, WP203, 2 April 2013, p. 11, disponibile al link: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

³⁶ Consiglio d'Europa, Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, STE n. 108 del 28 gennaio 1981, Strasburgo, consultabile al link: www.coe.int/t/t/web/conventions/full-list/-/conventions/treaty/108.

dati di carattere personale devono essere trattati « per finalità determinate ».

Tali norme segnano uno stretto legame tra il trattamento dei dati e la finalità per la quale sono stati raccolti. Ne segue come determinare le finalità del trattamento vuol dire ridurre e selezionare, tra le tante, una o più finalità specifiche in base alle quali i dati saranno trattati ³⁷. Ancora, come più evidente dal testo della Convenzione 108, questo implica che saranno vietati trattamenti e utilizzi dei dati per finalità diverse da quelle per le quali erano stati originariamente raccolti. Da qui il principio di “limitazione delle finalità”.

Il principio è chiaramente declinato anche nel Regolamento UE 2016/679, in particolare tra i principi applicabili al trattamento di dati personali di cui all'art. 5. Per quanto di interesse per questa trattazione, l'art. 5, paragrafo 1, lett. b), stabilisce che i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in un modo che non sia incompatibile con tali finalità (principio di limitazione della finalità). Ancora, i dati personali oggetto di trattamento devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle relative finalità (principio di minimizzazione dei dati).

Il principio di limitazione della finalità pone così in capo al titolare del trattamento tre obblighi: dovrà definire le finalità del trattamento prima del suo inizio; tali finalità devono essere individuate in modo specifico e ben definito, evitando espressioni generiche, ambigue o addirittura dubitative ³⁸; in conseguenza di ciò tali dati potranno essere usati per scopi aggiuntivi solo per finalità compatibili con quelle originarie mentre saranno vietati quelli per scopi incompatibili essendo questi non ricompresi ne sussumibili nell'originaria finalità e base di liceità dell'originario trattamento ³⁹.

La norma, mettendo in stretta correlazione tra loro da una parte la finalità del trattamento e gli obiettivi della raccolta dei dati e dall'altra l'effettivo e concreto utilizzo degli stessi ⁴⁰, mostra chiaramente come tale principio sia composto di due corollari: il criterio di specificazione delle finalità, con riferimento al fatto che i dati devono essere raccolti per finalità determinate, esplicite e legittime; e quello dell'uso compatibile, laddove prevede che i dati

³⁷ Cfr. L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati*, Milano, 2016, p. 98.

³⁸ Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, cit., p. 16: « a purpose that is vague or general, such as for instance “improving users’ experience”, “marketing purposes”, “IT-security purposes” or “future research” will - without

more detail - usually not meet the criteria of being specific ».

³⁹ FRA - CoE - ECHR - EDPS, *Handbook on European data protection law*, cit., p. 122 e ss.; L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 99.

⁴⁰ C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, cit., p. 110.

non possano essere trattati in modo incompatibile con la finalità precedentemente specificata ⁴¹.

Il criterio di specificazione delle finalità si pone come prerequisito per l'applicazione di altri principi in materia di protezione dei dati ⁴². Insieme al concetto di uso compatibile contribuisce al raggiungimento di valori quali la trasparenza, la certezza del diritto e la prevedibilità del trattamento. Entrambi mirano a proteggere l'interessato impostando dei limiti alle possibilità di trattamento del titolare, impedendo l'uso dei dati personali in modo inaspettato, inappropriato o altrimenti discutibile. Allo stesso tempo, la nozione di uso compatibile offre anche un certo grado di flessibilità per i titolari del trattamento dei dati. Infine, è sottinteso che il trattamento ulteriore deve perseguire scopi legittimi, concetto questo più ampio e che trascende quello di fondamento di liceità del trattamento ⁴³.

Il principio di limitazione delle finalità — o di “stretta finalità” ⁴⁴ — garantisce così la fiducia, la prevedibilità, la certezza del diritto nonché l'uso trasparente dei dati personali da parte dei titolari del trattamento. Ma oltre a ciò è particolarmente utile per la tematica ad oggetto laddove vieti che i dati raccolti per un certo trattamento siano poi usati per un ulteriore trattamento non compatibile con quello originario ⁴⁵. Così come vietati sarebbero tutti quei trattamenti, spesso diffusi in ambito big data, consistenti nel raccogliere e accumulare dati in eccesso sulla base dell'unico presupposto che potrebbero tornare utili in futuro ⁴⁶. Anzi, nella *ratio* del principio di limitazione delle finalità, in una logica proattiva, rientra proprio l'intento di scongiurare o limitare quanto più possibile tali abitudini degli operatori del mercato ⁴⁷.

In questo modo, il principio di limitazione delle finalità protegge gli interessati imponendo dei limiti all'utilizzo dei dati da parte dei titolari del trattamento. Ne segue come un principio cardine della disciplina *data protection* possa andare oltre il suo ambito naturale potendo agire anche in ottica antitrust: intervenendo in situazioni patologiche in cui un'azienda dominante abusi della sua posizione, anche a scapito dei consumatori/interessati ⁴⁸, agendo in settori terzi rispetto al proprio, alterando la concorrenza nei

⁴¹ Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, cit., p. 3.

⁴² Sui principi in materia di protezione dei dati personali si veda: FRA - CoE - ECHR - EDPS, *Handbook on European data protection law*, cit., p. 115 e ss.; L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 92 ss.

⁴³ Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, cit., p. 11 e ss e 20.

⁴⁴ F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit., p. 58.

⁴⁵ EDPS, *Privacy and competitiveness in the age of big data*, cit., § 22.

⁴⁶ V. BAGNOLI, *The big data relevant market*, cit., p. 84.

⁴⁷ FRA - CoE - ECHR - EDPS, *Handbook on European data protection law*, cit., p. 123.

⁴⁸ « In this perspective, the relevant

mercati e sfruttando dati ⁴⁹ e asset strategici già in loro possesso e preclusi ai concorrenti ⁵⁰.

Infine, il rilievo del principio di limitazione della finalità aumenta in un contesto economico caratterizzato sempre più dal ricorso ad algoritmi o sistemi di intelligenza artificiale. Questi sistemi permettono infatti di creare nuovi e ulteriori dati dall'elaborazione e dall'incrocio di quelli originariamente forniti, creando una seconda o anche terza "generazione" di dati personali. Così facendo tendono, per loro natura, a suggerire e rendere possibili utilizzi ulteriori, per ulteriori finalità, dei dati originariamente prestati per uno scopo specifico. Il principio di limitazione della finalità potrebbe così essere utile per attenuare o mitigare tale tendenza (c.d. *function creep*) e ridurre la perdita del controllo dei dati da parte degli interessati ⁵¹.

2.1. *Compatibilità del trattamento ulteriore.*

Non ogni trattamento di dati personali per scopi ulteriori è di per sé illecito. Al contrario, consentire entro certi limiti la possibilità di utilizzi ulteriori può costituire un valore ⁵².

Per poter quindi ritenere compatibile o meno un certo trattamento secondario sarà necessario condurre una valutazione caso per caso che tenga conto di alcuni fattori chiave ⁵³. Questi sono individuati nell'art. 6 paragrafo 4 GDPR e nel Considerando 50.

question is not whether or not big data is a source of a competitive advantage or a barrier to entry — neither of which is clearly prohibited as such — but whether a company may abuse its dominant position by refusing to grant third parties access to the big data it has collected. In other words, the question is whether the legal notion of refusal to supply covers also the refusal to supply access to big data ». Così G. PITRUZZELLA, *Big Data, Competition and Privacy*, cit., p. 22.

⁴⁹ Con riferimento all'utilizzo dei dati personali come corrispettivo dei servizi on line solo formalmente gratuiti si vedano G. GIANNONE CODIGLIONE, *I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la "consumizzazione" della privacy*, in *Diritto dell'informazione e dell'informatica*, fasc. 2, 2017, p. 418-425; V. BAGNOLI, *The big data relevant market*, in *Concorrenza e mercato*, fasc. 1, 1 gennaio 2016, p. 73-94.

⁵⁰ « For instance, processed data — based upon consent for specific purpose — could possibly be used for other purpose. In turn, this provision could raise some doubts on whether using data collected from third parties is unlawful from a competition point

of view ». Così A. MASSOLO, *Bundeskartellamt vs Facebook: time to refresh "GDPR's wall"?*, cit., p. 82.

⁵¹ EDPS, *Opinion 3/2018 on on line manipulation and personal data*, 19 March 2018, p. 15, consultabile al link: https://edps.europa.eu/data-protection/our-work/publications/opinions/on-line-manipulation-and-personal-data_en.

⁵² « The principle of purpose limitation — which includes the notion of compatible use — requires that in each situation where further use is considered, a distinction be made between additional uses that are compatible, and other uses, which should remain incompatible. The principle of purpose limitation is designed to offer a balanced approach: an approach that aims to reconcile the need for predictability and legal certainty regarding the purposes of the processing on one hand, and the pragmatic need for some flexibility on the other ». Così Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, cit., p. 5.

⁵³ C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, cit., p. 111; L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 100.

L'art. 6 paragrafo 4 prende in considerazione proprio l'ipotesi di un trattamento secondario e individua alcuni parametri sulla base dei quali verificare la compatibilità di quest'ultimo con la finalità del trattamento originale. In tal caso, a patto che tale trattamento secondario non trovi la sua base di liceità nel consenso dell'interessato o in un atto legislativo, la compatibilità della finalità del trattamento ulteriore con quella originaria dovrà essere valutata tenendo conto di elementi quali: il rapporto tra le finalità per le quali sono stati raccolti i dati e gli scopi dell'ulteriore trattamento; il contesto in cui sono stati raccolti e le ragionevoli aspettative degli interessati riguardo al loro ulteriore utilizzo; la natura dei dati personali e l'impatto dell'ulteriore trattamento sugli interessati; l'adozione da parte del titolare del trattamento di garanzie adeguate per prevenire qualsiasi impatto indebito sugli interessati ⁵⁴.

Affinché un trattamento di dati personali per finalità ulteriori rispetto a quelle per le quali erano stati inizialmente raccolti sia ammissibile, in quanto rispettoso del principio di limitazione della finalità, è necessario che quest'ultime finalità siano compatibili con quelle originarie. In questo modo, la questione si sposta sul generale concetto di "compatibilità" del trattamento ulteriore con quello originario ⁵⁵.

La valutazione della compatibilità dovrà essere condotta sulla base di un test formale e uno sostanziale. Il primo mira a verificare se le finalità ulteriori siano già rintracciabili in modo esplicito o implicito nelle finalità iniziali, mentre il secondo va oltre e indaga l'effetto delle ulteriori finalità sull'interessato, ossia come vengono recepite dall'interessato tenendo conto del contesto e degli altri elementi che caratterizzano la fattispecie specifica ⁵⁶.

La compatibilità dovrà inoltre essere valutata non solo alla luce dei già citati fattori chiave, ma anche con riferimento al concetto di "sostituibilità" utilizzato nell'applicazione delle regole di concorrenza per determinare quali prodotti possano essere considerati concorrenti nello stesso mercato ⁵⁷.

Per considerare un trattamento secondario, ulteriore o alternativo di dati come compatibile col trattamento originario bisognerà verificare anche se il trattamento secondario sia diretto o meno a una finalità sostitutiva di quella originaria. Nel caso in cui un'im-

⁵⁴ Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, WP203, 2 April 2013, p. 3.

⁵⁵ FRA - CoE - ECHR - EDPS, *Handbook on European data protection law*, cit., p. 123.

⁵⁶ L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 100 ss.

⁵⁷ EDPS, *Privacy and competitiveness in the age of big data*, cit., §23: « In the context of the digital economy, it is conceivable that a company might collect data for the purpose of providing a certain service in one market, and further process those data in order to compete in the provision of another service in a separate market ».

presa rielabori i dati già in suo possesso per fornire un nuovo servizio in un nuovo mercato, se tale servizio appartiene a un mercato del tutto separato o anche non concorrente con quello originario, allora vi potrebbe essere un certo margine per considerarlo non sostituibile con il servizio per il quale i dati sono stati originariamente raccolti. Pertanto, astrattamente parlando, si potrebbe concludere che i dati siano elaborati per scopi incompatibili, eventualmente anche all'insaputa degli interessati, e quindi non sarebbero utilizzabili perché in violazione del principio di limitazione della finalità del trattamento. Tale conclusione potrebbe essere più evidente nei casi in cui i due tipi di servizi siano percepiti dagli utenti in modo molto diverso⁵⁸. Stesso dicasi nel caso l'ulteriore finalità non possa essere considerata prevedibile perché non sufficientemente correlata allo scopo originario e quindi non soddisfa le ragionevoli aspettative degli interessati sul modo in cui saranno trattati i dati⁵⁹.

Per esempio, al netto delle caratteristiche concrete che possono portare un caso specifico a differire dal modello generale e astratto qui analizzato, dovrebbe in teoria essere precluso per un social network o una piattaforma attiva nel commercio elettronico usare gli stessi dati dei suoi utenti per offrire anche servizi finanziari, bancari o assicurativi⁶⁰.

Dunque, così come l'applicazione delle regole di concorrenza potrebbe aiutare a evidenziare ipotesi di violazione della legge sulla protezione dei dati, allo stesso tempo quest'ultima può essere utile per evitare distorsioni della concorrenza soprattutto nei casi che destano più preoccupazione, come quelli in cui un'impresa dominante in un mercato in cui i dati rappresentano un input significativo per l'attività di business controlli la raccolta dei dati dei consumatori.

3. USO SECONDARIO E TRASPARENZA.

Fermo restando che ogni trattamento deve fondarsi sulla più idonea base giuridica tra quelle previste dal GDPR, un tratta-

⁵⁸ EDPS, *Privacy and competitive-ness in the age of big data*, cit., § 58.

⁵⁹ G. PITRUZZELLA, *Big Data, Competition and Privacy*, cit., p. 19; Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, cit., p. 13.

⁶⁰ Ai servizi propriamente bancari si affiancano oggi i nuovi servizi di pagamento previsti dalla Direttiva (UE) 2015/2366 (c.d. PSD2). Questa prevede la possibilità per i *Payment initiation service provider*, ossia chi offre il servizio che dispone l'ordine di pagamento su richiesta dell'utente (art. 4, paragrafo 1, n. 15) e previo suo consenso

esplicito, di fornire tale servizio occupando una posizione intermedia tra il sito web del commerciante e la piattaforma di online banking della banca del pagatore per disporre pagamenti via Internet sulla base di bonifici (art. 66 - Considerando 27). Ancora, e sempre previo consenso dell'interessato, l'art. 67 permette un nuovo servizio accessorio, ossia il c.d. *account information service* (art. 4, paragrafo 1, n. 15), la possibilità di fornire all'utente informazioni consolidate relativamente ai suoi conti di pagamento (Considerando 28).

mento ulteriore ritenuto incompatibile non sarà sanabile semplicemente mutando in corso d'opera la base giuridica del trattamento ulteriore⁶¹ né ricorrendo retroattivamente alla base giuridica dell'interesse legittimo⁶². Diversamente e anche qui sulla base di una valutazione "case-by-case", l'inizio di un ulteriore trattamento se potenzialmente incompatibile col principio di finalità dovrà essere subordinato a tutte quelle valutazioni e operazioni tipiche di un nuovo ed autonomo trattamento, a partire dall'individuazione del corretto fondamento di liceità e dalla preventiva valutazione d'impatto sulla protezione dei dati personali (c.d. DPIA ex art. 35 GDPR)⁶³.

Rilevante in tale contesto è il principio di trasparenza di cui agli artt. 12 e ss. del Regolamento 2016/679⁶⁴, soprattutto in relazione alle informazioni che il titolare del trattamento dovrà fornire agli interessati per l'utilizzo ulteriore dei loro dati.

Tale principio si pone come centrale e, collegato al trattamento dei dati personali, sottopone all'attenzione del giurista criticità di non poco conto. Ed infatti la scarsa o nulla trasparenza può portare a fallimenti di mercato che riducono la concorrenza e la comparabilità di beni e servizi arrecando danno tanto alle imprese quanto ai cittadini⁶⁵. Problematiche queste che ben potrebbero essere risolte tramite un'applicazione integrata delle normative a tutela dei dati personali, della concorrenza e del consumatore.

Il principio di limitazione delle finalità trova nella trasparenza un ulteriore collegamento al concetto di responsabilità del titolare del trattamento⁶⁶, nonché a quell'*accountability*⁶⁷ intesa tanto come "responsabilizzazione" (art. 5, paragrafo 2, prima parte

⁶¹ Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, cit., p. 3.

⁶² Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, WP259 rev.01, 28 novembre 2017, p. 26.

⁶³ « data processing for incompatible use is allowed provided a new legal ground is available: if so, the further processing would be considered as a new data processing operation disconnected from the original purpose », così Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, cit., p. 11; cfr. L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 101.

⁶⁴ Sulla trasparenza si veda: FRA - CoE - ECHR - EDPS, *Handbook on European data protection law*, cit., p. 119 e ss e 122; L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 95 ss. Con riferimento al ruolo nell'informazione nell'ambito della c.d. *Behavioral Law and*

Economics si veda: G. GRISI, *Gli obblighi informativi quali rimedio dei fallimenti cognitivi*, in G. ROJAS ELGUETA, N. VARDI (a cura di), *Oltre il soggetto razionale. Fallimenti cognitivi e razionalità limitata nel diritto privato*, Roma, 2014, p. 59-73. Si veda anche E. BATTELLI, *La nuova disciplina degli obblighi informativi nei contratti con i consumatori*, in *Giurisprudenza italiana*, 2014, p. 2608-2619.

⁶⁵ W. KERBER, *Digital markets, data, and privacy: competition law, consumer law and data protection*, cit., p. 14 ss.

⁶⁶ Cfr. Gruppo di lavoro Articolo 29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della Direttiva 95/46/CE*, WP217, 9 aprile 2014, p. 50 ss.

⁶⁷ Con riferimento al principio di responsabilità (accountability) si vedano: R. CELELLA, *Il principio di responsabilizzazione: la novità del GDPR*, in *Cyberspazio e Diritto*, n. 60 (1-2 - 2018), p.

GDPR) tanto come “render conto” (art. 5, paragrafo 2, seconda parte GDPR).

In altre parole, prima di riutilizzare i dati raccolti per una finalità diversa, il titolare del trattamento dovrà prontamente informare l'interessato e fornirgli tutte le indicazioni necessarie⁶⁸, in maniera chiara e semplice, compresa la nuova base giuridica del trattamento⁶⁹. Ciò è anche chiarito nel Considerando 61 GDPR, secondo il quale: « Il titolare del trattamento, qualora intenda trattare i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, dovrebbe fornire all'interessato, prima di tale ulteriore trattamento, informazioni in merito a tale finalità diversa e altre informazioni necessarie ».

Tali norme si pongono quindi non solo l'obiettivo di informare l'interessato di un ipotetico diverso utilizzo dei propri dati, ma di evitare ogni ulteriore utilizzo che l'interessato non potrebbe ragionevolmente attendersi⁷⁰. « In altre parole, l'interessato non dovrebbe essere colto di sorpresa dalla finalità del trattamento dei dati personali che lo riguardano »⁷¹.

Ciò al fine di mettere in condizione l'interessato di poter adeguatamente valutare la compatibilità dell'ulteriore trattamento e delle garanzie fornite o se esercitare diritti come quello alla limitazione o all'opposizione al trattamento.

L'unica eccezione a quanto sopra riguarda l'ulteriore tratta-

211-224; L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, p. 34 e ss.; L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 232 e ss.; G. GIANNONE CODIGLIONE, *Risk-based approach e trattamento dei dati personali*, in S. SICA, V. D'ANTONIO, G. M. RICCIO (a cura di), *La nuova disciplina della privacy*, Padova, 2016, p. 70 ss.

⁶⁸ L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 99; FRA - CoE - ECHR - EDPS, *Handbook on European data protection law*, cit., p. 125; L. MONTUORI, M. SIANO, *Evoluzione del concetto di consenso informato nel mondo digitale e transizione del marketing tradizionale alle attuali sfide della profilazione*, in G. BUSIA, L. LIGUORI, O. POLICINO con M. BASSINI (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali: bilanci e prospettive*, Roma, 2016, p. 101 ss. Cfr. Art. 13 paragrafo 3 GDPR con riferimento alle “Informazioni da fornire qualora i dati

personali siano raccolti presso l'interessato” ma soprattutto l'art. 14 paragrafo 4 GDPR con riferimento alle “Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato” laddove i dati riutilizzati, sebbene tecnicamente non ottenuti presso terzi in quanto già in possesso del titolare, non sono comunque forniti direttamente dall'interessato.

⁶⁹ Particolarmente rilevante nella logica delle tecnologie Big Data è « l'obbligo per il titolare, che intenda trattare i dati anche per finalità diverse da quella per cui sono stati raccolti, di fornire all'interessato informazioni in merito alle nuove finalità e ogni ulteriore notizia circa il periodo di conservazione dei dati, i criteri utilizzati per determinare tale periodo e le modalità per esercitare i suoi diritti ». Così F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit., p. 24.

⁷⁰ L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 102.

⁷¹ Gruppo di lavoro articolo 29, *Linee guida sulla trasparenza ai sensi del regolamento 2016/679*, WP260 rev.01, 11 aprile 2018, p. 25, consultabili al link: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

mento dei dati personali « a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici » ⁷². La finalità di tali trattamenti, purché in conformità con le garanzie previste dall'art. 89 paragrafo 1 GDPR, è infatti considerata *ex lege* compatibile con quella iniziale. Non sarà quindi necessario rinvenire una nuova base giuridica del trattamento o, al limite, questa sarà rinvenibile nell'esecuzione di un compito di interesse pubblico di cui all'art. 6, paragrafo 1, lett. e) GDPR ⁷³.

Inoltre, altro elemento indispensabile per legittimare l'ulteriore trattamento dei dati personali è anche il fattore tempo. Ossia il titolare deve fornire tutte le informazioni rilevanti in modo tempestivo. Questo vuol dire non solo semplicemente prima dell'inizio dell'ulteriore trattamento ma che tra tale comunicazione e l'inizio del nuovo trattamento deve intercorrere un lasso di tempo ragionevole e necessario affinché l'interessato possa compiere le sue valutazioni. Quale sia questo lasso di tempo rientra nella scelta del titolare in base al principio di *accountability*. Così come rientra in questo principio anche l'essere in grado di dimostrare e giustificare le scelte compiute in termini di quali dati fornire e in che tempo. In generale però, tanto più è pervasivo e meno atteso il nuovo trattamento e tante più informazioni dovrà fornire il titolare in un periodo di tempo tanto più distante dall'inizio del nuovo trattamento ⁷⁴.

4. USO SECONDARIO E BASE GIURIDICHE DELL'ULTERIORE TRATTAMENTO.

Al fine di usare i dati già in suo possesso e incrociarli con quelli ottenuti dalla nuova attività, e quindi superare i vincoli che il principio di limitazione delle finalità pone a un trattamento secondario incompatibile, il titolare del trattamento è tenuto per prima cosa ad individuare una nuova base giuridica che legittimi un trattamento altrimenti vietato ⁷⁵. Questo sostanzialmente significa iniziare un nuovo trattamento per finalità diverse e, conseguentemente, con una nuova base giuridica.

Tra i fondamenti individuati dall'art. 6 GDPR, si potrebbe per esempio richiedere il consenso degli interessati ⁷⁶ oppure, qualora si riesca a provare i requisiti, fare ricorso al legittimo interesse.

⁷² E. LONGO, *I trattamenti nel settore dell'istruzione e a fini di ricerca (scientifica, storica, statistica)*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, p. 491-508; FRA - CoE - ECHR - EDPS, *Handbook on European data protection law*, cit., p. 124; L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 98.

⁷³ Gruppo di lavoro articolo 29, *Linee guida sulla trasparenza ai sensi del regolamento 2016/679*, cit., p. 24 ss.

⁷⁴ Gruppo di lavoro articolo 29, *Linee guida sulla trasparenza ai sensi del regolamento 2016/679*, cit., p. 25 ss.

⁷⁵ Cfr. L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 101.

⁷⁶ Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, cit., p. 27 ss.

Con riferimento al consenso ⁷⁷, oggi previsto dall'art. 6, paragrafo 1, lett. a) GDPR, questo è sicuramente lo strumento che più dà all'interessato il controllo sui propri dati ⁷⁸, anche grazie alla possibilità riconosciuta dall'art. 7, comma 3, GDPR di revocare il consenso in qualsiasi momento ⁷⁹.

Inoltre, come già visto, lo stesso art. 6, paragrafo 4 GDPR, fa riferimento al consenso dell'interessato. Tanto più che tale paragrafo sembrerebbe vedere con particolare favore il ricorso sia al consenso dell'interessato che ad « un atto legislativo dell'Unione o degli Stati membri che costituisca[no] una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1 ». Queste basi giuridiche, diversamente dalle altre, sembrerebbero addirittura esenti dalla necessità di tener conto di quegli ulteriori elementi necessari per valutare la compatibilità tra la finalità del trattamento secondario e quello originario. Questo attribuirebbe alla norma una portata a tal punto ampia da porre quasi in secondo piano la valutazione di compatibilità di cui si è parlato in precedenza ⁸⁰. La riduzione del rilievo del criterio di compatibilità, che ben potrebbe essere percepito come una riduzione della tutela dell'interessato, sembrerebbe essere dalla norma compensato da un lato dal maggior potere in termini di controllo sui propri dati che, come si vedrà, l'istituto del consenso almeno in teoria riconosce all'interessato, dall'altro dalla presenza di una previa valutazione legislativa del trattamento secondario ritenuto lecito se e nella misura in cui diretto a soddisfare interessi generali quali la sicurezza nazionale e pubblica, la prevenzione e il perseguimento di reati, ecc.

L'istituto del consenso è strettamente legato al principio di limitazione delle finalità di cui all'art. 5, paragrafo 1, lett. b)

⁷⁷ Cfr. FRA - CoE - ECHR - EDPS, *Handbook on European data protection law*, cit., p. 142 e ss.; L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, cit., p. 47 e ss.; Article 29 Working Party, *Parere 15/2011 sulla definizione di consenso*, WP187, 13 luglio 2011; L. MONTUORI, M. SIANO, *Evoluzione del concetto di consenso informato nel mondo digitale e transizione del marketing tradizionale alle attuali sfide della profilazione*, in G. BUSIA, L. LIGUORI, O. POLICINO con M. BASSINI (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali: bilanci e prospettive*, Roma, 2016, p. 101-126. Con riferimento al ruolo del consenso nei servizi online si veda anche G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Rivista trime-*

strale di diritto e procedura civile, fasc. 2, 2018, p. 411-440. Nell'ambito del merito creditizio si veda G. BIFERALI, *Big data e valutazione del merito creditizio per l'accesso al peer to peer lending*, in *Diritto dell'informazione e dell'informatica*, fasc. 3, 1 giugno 2018, p. 487-517.

⁷⁸ Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, cit., p. 3.

⁷⁹ « se sceglie di basarsi sul consenso per ogni parte del trattamento, il titolare del trattamento deve essere preparato a rispettare tale scelta e interrompere il trattamento in caso di revoca del consenso », così Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, cit., p. 26.

⁸⁰ F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit., p. 58 ss.

GDPR. Infatti, il presupposto di un consenso valido è proprio la determinazione della finalità del trattamento in modo specifico, esplicito e legittimo⁸¹. In altre parole, il consenso si pone come strumento per applicare e garantire il principio di limitazione della finalità, operando come argine contro l'ampliamento progressivo o la commistione della finalità originaria e contribuendo a ridurre il fenomeno del “*function creep*”⁸², ossia l'uso non previsto dei dati dell'interessato da parte del titolare o di terzi⁸³.

Il consenso sembrerebbe quindi la base giuridica più adeguata per legittimare l'uso secondario di dati essendo lo strumento che più rimette allo stesso interessato la scelta di autorizzare il trattamento dei propri dati⁸⁴.

Ciò non toglie che l'istituto del consenso rimane tutt'oggi un'arma a doppio taglio per l'interessato. È infatti ormai comprovata la tendenza dell'interessato, o dell'utente di Internet in generale, a non leggere le informative e concedere il proprio consenso con eccessiva superficialità⁸⁵. Inoltre, l'ottenimento di un consenso effettivamente “libero, specifico, informato e inequivocabile” presuppone non solo un corretto adempimento da parte del titolare del trattamento del suo dovere di informazione e trasparenza⁸⁶, ma anche un adeguato livello di conoscenza da parte dell'interessato del contesto generale coinvolgente il trattamento dei dati. Un livello almeno tale da riequilibrare la sempre più ampia asimmetria informativa tra il titolare/professionista e l'interessato/consumatore/utente. Ancora, al fine di permettere un effettivo esercizio del diritto dell'interessato all'autodeterminazione informativa, sarà anche opportuno affiancare un'attività informativa complementare da parte dei pubblici poteri⁸⁷.

Sebbene queste siano condizioni non facili da realizzare, ciò non

⁸¹ Con riferimento alla necessità di un consenso specifico si veda: G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi di rete*, in *Riv. Trim. dir. proc. civ.*, 2018, p. 434; G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 286-287.

⁸² Secondo il WP29 il principio di limitazione della finalità sarebbe diretto proprio alla riduzione del fenomeno della “*mission*” o “*function creep*”. Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, cit., p. 4.

⁸³ Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, cit., p. 13.

⁸⁴ F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit., p. 16 ss.

⁸⁵ EDPS, *Privacy and competitiveness in the age of big data*, cit., §§76 e ss.; W. KERBER, *Digital markets, data, and pri-*

vacy: competition law, consumer law and data protection, cit., p. 12 e ss.; D.J. SOLOVE, *Introduction: Privacy self-management and the consent dilemma*, in *Harvard Law Review*, 2013, p. 1880 anche disponibile al seguente link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.

⁸⁶ Cfr. E. BATTELLI, *Interpretatio contra proferentem e trasparenza contrattuale*, in *Contratto e impresa*, 2017, fasc. 1, p. 194-232; E. BATTELLI, *La nuova disciplina degli obblighi informativi nei contratti con i consumatori*, in *Giurisprudenza italiana*, 2014, p. 2608-2619.

⁸⁷ « D'altra parte l'efficacia del consenso informato nel caso, per esempio dei trattamenti medico-sanitari, dipende anche dalla circostanza che il paziente non viene “lasciato solo” né nella formazione del suo convincimento né nel momento della scelta responsabile, potendo avvantaggiarsi della

dovrebbe comunque spingere il titolare ad approfittarne, pena la riduzione della fiducia nello sviluppo tecnologico e nel mercato unico digitale. Il ricorso al consenso come base giuridica, infatti, non legittima il titolare ad un adempimento solo formale degli obblighi normativi. Soprattutto non lo autorizza a non rispettare principi come quelli di correttezza, proporzionalità e necessità del trattamento, nonché la qualità dei dati e il principio di minimizzazione e non lo legittima, quindi, a raccogliere dati non necessari per il perseguimento della finalità dichiarata ⁸⁸.

La necessità e l'importanza di ottenere un consenso autentico è di immediata percezione se si pensa alla sanzione conseguente alla raccolta di dati sulla base di un consenso invalido o illusorio. Ossia, tale consenso non costituirà un'idonea base di legittimità del trattamento, rendendo illecita l'attività e inutilizzabili i dati raccolti, con ciò che ne consegue in termini di responsabilità.

Nei casi in cui l'asimmetria informativa, o lo squilibrio di potere tra titolare e interessato sia tale da non rendere possibile un consenso effettivo, o in generale il consenso non sia lo strumento più idoneo per quel particolare trattamento secondario, bisognerà fare ricorso ad altre basi di liceità del trattamento.

Tra questi, il titolare del trattamento potrebbe ritenere di fondare il trattamento secondario di dati sulla base del legittimo interesse ⁸⁹ proprio o di terzi di cui all'art. 6, paragrafo 1, lett. f) GDPR ⁹⁰, in conformità al principio di *accountability* e previo il "test comparativo" richiesto dalla norma.

Proprio il ricorso a tale base potrebbe rendere lecito l'ulteriore trattamento dei dati. Ciò però a condizione che si rispettino i requisiti sottesi al ricorso a tale fondamento di liceità, a partire dalla valutazione dello stretto legame tra interesse e finalità ⁹¹.

Oltre a ciò, l'interesse deve essere legittimo, ossia lecito ai sensi della normativa europea e nazionale, necessario per il persegui-

relazione con il medico ». Così C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, cit., p. 120. Sulle difficoltà incontrate dagli utenti nel proteggere la loro privacy on line si veda W. KERBER, *Digital markets, data, and privacy: competition law, consumer law and data protection*, cit., p. 7 ss e 12 ss.

⁸⁸ Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, cit., p. 4.

⁸⁹ F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit., p. 58.

⁹⁰ FRA - CoE - ECHR - EDPS, *Handbook on European data protection law*, cit., p. 155 e ss.; L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*,

cit., p. 295 e ss.; Gruppo di lavoro Articolo 29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della Direttiva 95/46/CE*, WP217, 9 aprile 2014, p. 50 ss., consultabile al link: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

⁹¹ « In data protection discourse, "purpose" is the specific reason why the data are processed: the aim or intention of the data processing. An "interest", on the other hand, is the broader stake that a controller may have in the processing, or the benefit that the controller derives - or that society might derive - from the processing », così Gruppo di lavoro Articolo 29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della Direttiva 95/46/CE*, cit., p. 28.

mento dell'interesse del titolare del trattamento e superare il test comparativo. Ossia, l'interesse legittimo del titolare o di soggetti terzi deve essere ritenuto prevalente rispetto agli interessi, diritti e libertà fondamentali dell'interessato ⁹².

Così facendo, fermo il rispetto degli obblighi generali imposti dal GDPR, il titolare eviterebbe l'eventualità che l'interessato non acconsenta al trattamento o revochi il consenso ma si esporrebbe a un più pervasivo scrutinio da parte delle autorità di controllo sul corretto bilanciamento dei suoi interessi con quelli degli interessati. Inoltre, il ricorso al legittimo interesse come base giuridica non attenua gli oneri che il GDPR pone in capo al titolare del trattamento né lo pone al riparo dall'esercizio del diritto di opposizione da parte dell'interessato o, in alcuni casi, come si vedrà meglio in seguito, della stessa revoca quale ulteriore garanzia per l'interessato ⁹³.

In definitiva, tanto l'informazione e le norme di trasparenza quanto il ricorso a una nuova base giuridica del trattamento, prima del riutilizzo dei dati, poiché configura la creazione di un nuovo trattamento, permettono di sganciare il trattamento secondario incompatibile da quello originale, superando così il vincolo del principio di limitazione della finalità ⁹⁴. Non si dimentichi infatti che scopo della convergenza di tali norme con quelle a tutela della concorrenza non è vietare il riutilizzo di dati ma subordinarlo alle norme che garantiscono la correttezza del trattamento e il rispetto dei diritti coinvolti. Scopo di questa trattazione è allora indagare quali possono essere gli abusi e quali i rimedi e come istituti che vertono sul ruolo dell'informazione e del controllo sui dati da parte degli interessati possano ristabilire la legalità di un trattamento.

Ad essere vietato non è infatti qualunque trattamento secondario ma solo quello per finalità incompatibili con quelle originarie. Ciò è in linea con il bilanciamento che l'art. 1 GDPR fa tra protezione delle persone fisiche e libera circolazione dei dati. La protezione dei dati personali, ancorché rivesta valenza fondamentale, non è un diritto assoluto. Al contrario è un diritto che deve essere bilanciato con gli altri interessi coinvolti valorizzandone la sua funzione sociale ⁹⁵. Solo un adeguato e costante bilanciamento di questi interessi permetterà sia la tutela delle persone, sia il

⁹² Gruppo di lavoro Articolo 29, *Parere 6/2014 sul concetto di interesse legittimo*, cit., p. 30 ss.

⁹³ Gruppo di lavoro Articolo 29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della Direttiva 95/46/CE*, cit., p. 53.

⁹⁴ « data processing for incompatible use is allowed provided a new legal ground

is available: if so, the further processing would be considered as a new data processing operation disconnected from the original purpose ». Così Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, cit., p. 30; L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 101.

⁹⁵ Cfr. Considerando 4; W. KERBER, *Digital markets, data, and privacy: compe-*

funzionamento del mercato e, in ultima analisi, la fiducia nei mercati ⁹⁶.

Tanto più, tale interpretazione risulterà condivisibile se si pensa al fatto che il paragrafo 3 dello stesso articolo 1 ricorda che: « La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali ».

5. IL CASO FACEBOOK/WHATSAPP.

Applicando quando detto al caso dell'unione di più banche dati per svolgere un nuovo servizio si potrebbe giungere alle seguenti conclusioni. Se l'impresa X, nel momento in cui entra nel mercato Y basasse la sua attività sull'acquisizione di nuovi dati e, quindi, su un nuovo trattamento, *nulla quaestio*. Se invece intendesse utilizzare i dati già raccolti anche per la nuova attività nell'ulteriore mercato questo non gli sarebbe possibile perché potrebbe violare il principio di limitazione delle finalità ⁹⁷.

Ipotesi assimilabile a quella dell'ingresso in un nuovo mercato o del lancio di un nuovo servizio, ancorché caratterizzata da modalità operative diverse, si ha quando un unico titolare del trattamento che offre servizi differenti decidesse di unire i dati raccolti dai due trattamenti per aumentare il rendimento di uno o di entrambi i servizi.

A quest'ultima ipotesi si avvicina il caso Facebook/Whatsapp, questione che ha prodotto e continua a produrre numerosi rilievi da parte di autorità e enti diversi, sia in ambito *data protection* che di concorrenza e tutela del consumatore.

Il caso ⁹⁸ è stato inizialmente affrontato dalla Commissione Europea nel 2014, con riferimento all'operazione di acquisizione dell'applicazione di messaggistica Whatsapp da parte di Facebook ⁹⁹.

Sebbene la Commissione abbia avuto cura nel distinguere e nel non trattare le questioni più propriamente di *data protection* ¹⁰⁰, tra quelle affrontate vi è anche la possibilità che Facebook, integrando i due servizi, potesse usare i dati raccolti da WhatsApp

tion law, consumer law and data protection, cit., p. 14 ss.

⁹⁶ « privacy is an important element of trust and trust in digital services is necessary for on line markets to work smoothly and to be an engine of growth and competitiveness ». Così G. PITRUZZELLA, *Big Data, Competition and Privacy, cit.*, p. 26.

⁹⁷ Cfr. L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo, cit.*, p. 100.

⁹⁸ Oltre a Facebook/Whatsapp si veda anche il più recente caso Apple/Shazam, case number M.8788, September 2018 e il caso Microsoft/Linkedin, case Case M.8124, december 2016.

⁹⁹ Facebook/WhatsApp, case number M.7217, 3 October 2014: http://europa.eu/rapid/press-release_IP-14-1088_en.htm.

¹⁰⁰ Commission decision, Case M.7217 - Facebook/WhatsApp, punto 164.

per rafforzare la posizione di Facebook nel mercato dell'*online advertising* ¹⁰¹.

Se applicato a questo contesto, il principio di limitazione della finalità potrebbe essere utile per tenere distinti i data base prodotti dai due servizi, e quindi trattamenti, diversi. Nonché potrebbe essere utile per valutare se l'acquisizione di una società e dei dati da questa detenuti possa alterare la concorrenza in un certo mercato. Ciò presuppone un'attenta ricognizione dei fatti, del rapporto tra i soggetti coinvolti, dei servizi e dei trattamenti effettuati nonché l'analisi dei mercati rilevanti ¹⁰².

Nella sua istruttoria la Commissione europea rilevava come sia Facebook che WhatsApp siano attivi nel mercato dei "*consumer communication app*" ma che questo mercato abbia comunque degli ambiti di sovrapposizioni con quello dei "*social networking app*". Quest'ultimo è il mercato nel quale Facebook, specialmente con riferimento alla piattaforma digitale, ha il suo *core business*, ma lo stesso è attivo, al pari di Whatsapp, anche nel mercato dei "*consumer communication app*" con riferimento all'app di messaggistica Facebook Messenger, sebbene i due servizi siano diversi e la Commissione li abbia ritenuti non in concorrenza tra loro ¹⁰³. Inoltre, e soprattutto, Facebook è attivo anche nell'*online advertising market*, settore in cui invece WhatsApp è assente ¹⁰⁴.

Una prima e astratta applicazione del principio di limitazione delle finalità a questa fattispecie, con riferimento alla condivisione dei dati prodotti dall'interazione con WhatsApp (ammesso che l'utilizzo di WhatsApp produca dati economicamente rilevanti, eventualità esclusa dalla Commissione) al fine di migliorare la posizione di Facebook (sicuramente con riferimento alla Facebook Messenger, in una certa misura eventualmente anche con riferimento alla piattaforma social), potrebbe portare a ritenere

¹⁰¹ Commission decision, Case M.7217 - Facebook/WhatsApp, punti 164 ss.

¹⁰² Sul concetto di mercato rilevante si veda R. WHISH - D. BAILEY, *Competition law*, 9th ed. Oxford: Oxford University Press, 2018. Con riferimento ai big data si veda: ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 204 ss. Non semplice appare la delimitazione del relativo mercato rilevante con riferimento ai big data e si preferisce escludere l'individuazione di un mercato rilevante dei big data *tout court* ma piuttosto distinguere caso per caso tra i più mercati relativi ai servizi basati sull'utilizzo di big data. Cfr. G. PIRUZZELLA, *Big Data, Competition and Privacy*, cit., p. 15 e ss.; F. DI PORTO, *La rivoluzione big data. Un'introduzione*, in *Concorrenza e mercato*, fasc. 1, 1 gennaio

2016, p. 3 ss. Secondo V. BAGNOLI, *The big data relevant market*, cit., p. 73-94, si può individuare un mercato rilevante dei big data al fine di descrivere il quadro complessivo degli aspetti significativi dal punto di vista del diritto della concorrenza. Tale mercato sarebbe composto di tre segmenti: (i) *Big Data capture*, comprendente la raccolta tanto dei dati; (ii) *Big Data storage*; (iii) *Big Data analytics*. Per l'esame dei mercati rilevanti in relazione alle "*attention e matching platforms*" si veda G. MUSCOLO, *Big data e concorrenza. Quale rapporto?*, cit., p. 175 e ss.; M. GAMBARO, *Big data, mercato e mercati rilevanti*, cit., p. 205 ss.

¹⁰³ Commission decision, Case M.7217 - Facebook/WhatsApp, punti 101, 102, 103, 153 e ss. e 158.

¹⁰⁴ Commission decision, Case M.7217 - Facebook/WhatsApp, punto 71.

lecito l'ulteriore trattamento dei dati personali da parte dell'altro fornitore di *consumer communication app*, in quanto tale trattamento potrebbe essere considerato compatibile con le finalità del trattamento originario. Ciò se non altro perché, i due soggetti svolgono servizi simili, sostituibili e probabilmente anche concorrenti con riferimento a Fb Messenger. In questo senso le finalità del trattamento dei due servizi coinciderebbero. Lo stesso potrebbe essere l'esito anche nel rapporto tra una *consumer communication app* e una *social networking app* (in questo caso facciamo riferimento alla piattaforma social di Facebook), laddove i reciproci ambiti di sovrapposizione potrebbero spingere a considerare l'ulteriore trattamento dei dati prodotti da uno dei due servizi come compatibile con le finalità originarie. Stesso risultato ma ricorrendo alla base giuridica dell'interesse legittimo si otterrebbe in relazione al riutilizzo dei dati nel mercato dell'*online advertising* poiché, come previsto dal Considerando 47, l'attività di marketing può essere considerato un interesse legittimo del titolare del trattamento.

Diversamente, se invece si valorizzasse la percezione che i consumatori/utenti hanno dei due servizi come sostanzialmente diversi, come anche ritenuto dalla Commissione¹⁰⁵, allora l'applicazione del principio di limitazione delle finalità potrebbe avere risultati opposti.

La Commissione, nella sua veste di *competition authority*, con riferimento alla possibilità di Facebook di rafforzare la sua posizione nel mercato della pubblicità on line tramite i dati di WhatsApp, ha formulato due teorie del danno. La prima fa riferimento alla possibilità di introdurre spazi pubblicitari all'interno dell'app di WhatsApp. La seconda all'utilizzo di WhatsApp come potenziale fonte di acquisizione dei dati per migliorare l'accuratezza della pubblicità mirata ("targettizzata") di Facebook¹⁰⁶. Il primo caso è valutato come poco probabile perché rischierebbe di produrre effetti negativi spingendo gli utenti ad abbandonare WhatsApp per uno degli altri numerosi servizi di messaggistica¹⁰⁷. Il secondo invece potrebbe trovare applicazione solo in seguito al cambiamento della *privacy policy* di WhatsApp, al fine di prevedere la raccolta e il trattamento dei dati personali diversi dal nome e dal numero di telefono (già raccolti dall'app), e soprattutto dopo la realizzazione di sistemi che permettano la possibilità di stabilire una corrispondenza automatizzata tra gli account degli utenti di Facebook e quelli di WhatsApp¹⁰⁸. In base alla documentazione nella disponibilità della Commissione però

¹⁰⁵ Commission decision, Case M.7217 - Facebook/WhatsApp, punti 52 e ss e 103.

¹⁰⁶ Commission decision, Case M.7217 - Facebook/WhatsApp, punto 167.

¹⁰⁷ Commission decision, Case M.7217 - Facebook/WhatsApp, punti 172 e ss

¹⁰⁸ Commission decision, Case M.7217

queste attività non sarebbero nelle intenzioni di Facebook e comunque non comporterebbero criticità concorrenziali laddove la quote di mercato ottenute dell'entità risultate dalla concentrazione Facebook/WhatsApp nel settore della pubblicità on line sarebbe comunque non significativa ¹⁰⁹. In conclusione, la Commissione dichiara l'operazione di concentrazione ad oggetto compatibile con il mercato interno ¹¹⁰.

La situazione così descritta muta però nel 2016 quando WhatsApp modifica la sua informativa privacy prevedendo la raccolta di dati personali e nel 2017 la Commissione europea torna nuovamente sulla questione in sede sanzionatoria. In tale contesto la Commissione sanziona Facebook con una multa di 110 milioni di euro per aver fornito indicazioni inesatte o fuorvianti con riferimento alla sua effettiva possibilità di stabilire una corrispondenza automatizzata tra gli account degli utenti di Facebook e quelli di WhatsApp, mescolando così i dati dei due servizi e unendo i numeri di telefono all'identità degli utenti Facebook ¹¹¹.

La questione ha così sollecitato l'intervento anche delle Autorità di controllo in materia di protezione dei dati personali, riunite nell'ambito del Gruppo Articolo 29 (o "WP29", oggi sostituito dal Comitato europeo per la protezione dei dati ex art. 68 GDPR).

Con una lettera aperta del 24 ottobre 2017, il WP29 riassume la sua posizione in merito alle modifiche apportate da WhatsApp ai suoi *Terms of Service* e *Privacy Policy* e annuncia la creazione di una task force con le Autorità di controllo europee guidata dall'Autorità inglese: l'*Information Commissioner's Office* ¹¹².

Innanzitutto il WP29 sottolinea la carenza di una adeguata informazione sulla natura e le finalità della condivisione dei dati personali di WhatsApp con il gruppo Facebook. Le criticità si assestano quindi sulla: base giuridica del trattamento, in quanto sia il consenso che il legittimo interesse non sarebbero validi, il primo perché non libero, non corrispondente ai requisiti normativi e in più "pre-spuntato", costringendo così l'utente ad un'azione

- Facebook/WhatsApp, punti 180 e ss., in particolare 185.

¹⁰⁹ Commission decision, Case M.7217 - Facebook/WhatsApp, punto 189.

¹¹⁰ ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 224 ss, rileva come proprio riscontrando la presenza di numerosi e importanti operatori capaci di collezionare dati permette di escludere che la concentrazione ad oggetto potesse comportare un danno al benessere del consumatore.

¹¹¹ European Commission, *Press release: Mergers: Commission fines Facebook*

€110 million for providing misleading information about WhatsApp takeover, Brussels, 18 May 2017, Caso M.8228 - Facebook/WhatsApp http://europa.eu/rapid/press-release_IP-17-1369_en.htm. Una sintesi della decisione della Commissione è disponibile al link: [https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52017M8228\(03\)&from=IT](https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52017M8228(03)&from=IT).

¹¹² Letter of the Chairwoman of Article 29 Data Protection Working Party, Isabelle Falque-Pierrotin, to WhatsApp, Brussels, 24 October 2017, disponibile al link: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47964.

positiva per non acconsentire al trattamento secondo un meccanismo di *opt-out*, il secondo perché non sembrerebbe essere soddisfatto il test comparativo e gli altri requisiti richiesti dalla normativa sull'interesse legittimo; sulle informazioni agli utenti gravemente carenti, fuorvianti e che ingenerano nell'utente la convinzione che senza il consenso alla condivisione dei dati il servizio non sarebbe stato più disponibile (c.d. "*take it or leave it approach*"); sulla mancata previsione di un diritto di recesso.

Infine e con implicito riferimento al principio di limitazione della finalità, il WP29 rileva che la condivisione dei dati debba rispondere a uno scopo specifico e definito nonché necessario e proporzionato alle circostanze. In conseguenza di ciò, ogni condivisione di dati deve essere strettamente adattata e limitata a quanto necessario per raggiungere lo scopo specifico in questione.

Successivamente si registra l'intervento anche delle altre Autorità di controllo. Il 4 ottobre 2018, all'esito di una lunga istruttoria iniziata nel settembre 2016, il Garante per la Protezione dei Dati Personali vieta a WhatsApp di comunicare i dati dei propri utenti a Facebook¹¹³. L'analisi del Garante considera Facebook e WhatsApp quali autonomi titolari del trattamento con la conseguenza che il trasferimento di dati tra loro è qualificato come comunicazione a terzi. Poiché questa operazione può essere effettuata lecitamente solo con il consenso informato degli interessati (o su altra idonea base giuridica del trattamento) è su questo che si incentra l'analisi del Garante. Nello specifico il Garante reputa l'informativa relativa alla condivisione non rispettosa del principio di correttezza e non idonea al rispetto dei requisiti previsti dalla normativa¹¹⁴. Ancora, il Garante non ritiene idoneo il ricorso all'interesse legittimo del titolare del trattamento¹¹⁵. Con riferimento invece ad ulteriori profili di criticità, qualora WhatsApp intenda comunque comunicare i dati a Facebook per la finalità di "*targeted Advertising Purpose*"¹¹⁶, sulla base di un nuovo e valido consenso o di altra base giuridica, in considerazione delle modifiche apportare dal Regolamento UE 2016/679, l'attività di vigilanza spetterà all'Autorità di controllo Irlandese quale "autorità capofila". In questo contesto ben potrebbe tro-

¹¹³ Provvedimento del Garante per la Protezione dei dati personali n. 462 del 4 ottobre 2018, doc. web n. 9058572, *WhatsApp: divieto di cessione dei dati degli utenti a Facebook*, disponibile al link: www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9058572.

¹¹⁴ Provvedimento GPDP n. 462 del 4 ottobre 2018, punto 4, lett. a) e b).

¹¹⁵ Provvedimento GPDP n. 462 del 4 ottobre 2018, punto 4, lett. c).

¹¹⁶ Il Garante rileva come trattamento

dei dati personali raccolti tramite WhatsApp da parte di Facebook sarebbe stato riconducibile a tre finalità: a) "*Business Analysis Analytics*": ossia la de-duplicazione degli account sulle varie app del gruppo (WhatsApp, Facebook e Instagram); b) "*System Security Purpose*": ossia finalità di sicurezza e antispam; c) "*Targeted advertising Purpose*": ossia l'utilizzo dei dati degli utenti WhatsApp per promuovere prodotti e inserzioni pubblicitarie sul social network Facebook.

vare applicazione anche il principio di limitazione della finalità con riferimento all'ulteriore trattamento dei dati di WhatsApp con la finalità di attribuire vantaggi a Facebook nel mercato dell'*online advertising*.

Contestualmente, l'acquisizione di Whatsapp da parte di Facebook è stata inoltre esaminata, nel nostro ordinamento, anche dall'Autorità Garante della Concorrenza e del Mercato dal punto di vista della tutela del consumatore¹¹⁷. L'AGCM ha emanato infatti due provvedimenti, il primo¹¹⁸ avente ad oggetto l'accertamento della pratica commerciale scorretta integrata dall'aver indotto gli utenti di WhatsApp Messenger ad accettare integralmente i nuovi termini di utilizzo¹¹⁹ e in particolare la condivisione dei propri dati con Facebook paventando l'impossibilità per l'utente di proseguire nell'uso dell'applicazione, il secondo¹²⁰ dichiarando la vessatorietà di alcune clausole contrattuali imposte agli utenti/consumatori¹²¹. Si evince quindi come, la stessa fattispecie che ha visto l'intervento sanzionatorio da parte del Garante per la Protezione dei Dati Personali ha suscitato anche quello dell'Autorità Garante della Concorrenza e del Mercato. Stessa fattispecie ma esaminata da punti di vista diversi e che ben si presterebbe ad una valutazione complessiva in ottica convergente tra le discipline coinvolte. Il rilievo della disciplina sulla privacy deriva infatti sia dal riconoscimento del valore rivestito dai dati personali nell'attività economica delle piattaforme digitali, cosa che ha indotto Facebook a forzare il consenso — istituto di per sé già rilevante per entrambe le normative coinvolte — alla

¹¹⁷ G. RESTA, *Digital platforms and the law*, cit., p. 237 ss.

¹¹⁸ Provvedimento AGCM PS10601 dell'11 maggio 2017, disponibile al link: www.agcm.it/dotcmsDOC/allegati-news/PS10601_scorrsanz_omi.pdf Si veda anche il comunicato stampa: PS10601 CV154 - Sanzione da 3 milioni di euro per WhatsApp, ha indotto gli utenti a condividere i loro dati con Facebook, 12 maggio 2017, disponibile al link: www.agcm.it/media/dettaglio?id=61dde0b6-d8aa-4a34-b9c8-aeb9a39ee71e.

¹¹⁹ Con riferimento al rilievo e l'importanza assunta dai cc.dd. *Terms and conditions* si vedano: S.F. BONETTI, *La tutela del consumatore nei contratti gratuiti di accesso ad Internet: i contratti dei consumatori e la privacy tra fattispecie giuridiche e modelli contrattuali italiani e statunitensi*, in *Diritto dell'informazione e dell'informatica*, 2002, fasc. 6, p. 1087-1140; M. GRANIERI, *Le clausole ricorrenti nei contratti dei social networks dal punto di vista della disciplina consumeristica dell'Unione europea*, in *AIDA*, pt. 1, 2011, p. 125-143; A.R. POPOLI, *Social network e concreta pro-*

tezione dei dati sensibili: luci ed ombre di una difficile convivenza, in *Diritto dell'informazione e dell'informatica*, fasc. 6, 2014, p. 981-1017.

¹²⁰ Provvedimento AGCM CV154 dell'11 maggio 2017, disponibile al link: www.agcm.it/dotcmsDOC/allegati-news/CV154_vessestratto_omi.pdf Si veda anche il comunicato stampa: PS10601 CV154 - Sanzione da 3 milioni di euro per WhatsApp, ha indotto gli utenti a condividere i loro dati con Facebook, 12 maggio 2017, disponibile al link: www.agcm.it/media/dettaglio?id=61dde0b6-d8aa-4a34-b9c8-aeb9a39ee71e.

¹²¹ L'AGCM ha dichiarato la vessatorietà delle clausole che stabilivano, per esempio: esclusioni e limitazioni di responsabilità in capo a WhatsApp; la possibilità di interruzioni unilateralmente del servizio; il diritto di WhatsApp di risolvere il contratto in qualsiasi momento e per qualsiasi motivo; il diritto di WhatsApp di introdurre modifiche unitamente alla previsione del "silenzio assenso" da parte dell'utente. Cfr. Provvedimento AGCM CV154, cit.

condivisione dei dati tra le due piattaforme, sia con riferimento alla disciplina delle clausole vessatorie. Con riferimento a queste ultime, la rilevanza della normativa *data protection* è, tra le altre, particolarmente evincibile dalla clausola che prevedeva la risoluzione unilaterale del contratto da parte di Facebook facendo però salva la possibilità per quest'ultimo di « trasferire le informazioni dell'utente alle proprie affiliate, agli aventi causa o a un nuovo proprietario »¹²². Anche qui, un istituto tipico della normativa *data protection*, il corretto trasferimento di dati a terzi, diventa elemento di analisi utile per altre discipline, in questo caso le norme a tutela del consumatore.

Ma soprattutto, importante in tal senso è la recente pronuncia dell'AGCM¹²³ che ha sanzionato Facebook per due pratiche commerciali scorrette (ingannevole la prima e aggressiva la seconda¹²⁴) aventi ad oggetto la raccolta, lo scambio con terzi e l'utilizzo, a fini commerciali, dei dati personali degli utenti-consumatori, incluse le informazioni sui loro interessi on line. Significativo, per un'analisi convergente tra tutela dei dati personali e tutela dei consumatori, è rilevare il fatto come oggetto di analisi da parte dell'AGCM siano fenomeni tipicamente di *data protection*, quali appunto la raccolta, lo scambio e il trattamento di dati personali, integranti però anche pratiche commerciali ingannevoli e aggressive. In tale circostanza si potrebbe anche rilevare come, allo stato e visti anche i precedenti della stessa AGCM, il ricorso alla normativa sulla privacy in ottica convergente abbia prodotto migliori e immediati agganci più per la normativa a tutela del consumatore che per quella sulla concorrenza. Infine, può essere significativo rilevare che in questo nuovo caso l'AGCM abbia ripreso e analizzato le criticità sollevate dal WP29 nella lettera del 24 ottobre 2017. In questo modo l'AGCM chiude il cerchio aperto dal WP29 completandone e integrandone le valutazioni e, soprattutto, rafforzando un "dialogo" tra autorità operanti in settori differenti ma sempre più interrelati.

Con riferimento alla prima pratica contestata a Facebook, in quanto violativa degli artt. 21 e 22 del d.lgs. 206/2005, tale professionista avrebbe indotto ingannevolmente gli utenti consumatori a registrarsi sulla piattaforma non informandoli adeguatamente e immediatamente, in fase di attivazione dell'account, dell'attività di raccolta con intento commerciale dei loro dati e delle sottese finalità remunerative, enfatizzando invece la gratuità

¹²² Provvedimento AGCM CV154, cit., punto 80.

¹²³ Provvedimento AGCM PS11112 del 7 dicembre 2018, che ha visto sanzionare Facebook per pratiche commerciali scorrette per un totale di 10 milioni di euro, è

disponibile al link: www.agcm.it/media/comunicati-stampa/2018/12/Uso-dei-dati-degli-utenti-a-fini-commerciali-sanzioni-per-10-milioni-di-euro-a-Facebook.

¹²⁴ Provvedimento AGCM PS11112, punto 47.

dell'utilizzo della piattaforma ¹²⁵. Si evidenzia qui e si riconosce il valore economico e commerciale dei dati, smascherando ufficialmente la diffusa credenza della gratuità di servizi online che in realtà sono retribuiti con lo scambio di dati personali ¹²⁶.

Di maggior interesse per l'ottica convergente adottata dalla presente trattazione è la seconda pratica contesta quale condotta specificatamente aggressiva ex artt. 24 e 25 d.lgs. 206/2005, quella secondo la quale il professionista realizza una trasmissione automatica dei dati degli utenti dalla piattaforma ai siti web/app di terzi e viceversa, senza preventivo consenso dell'interessato, per l'uso degli stessi a fini di profilazione e commerciali. Questo perché Facebook crea un meccanismo di *opt-out* per cui il consenso dell'utente alla condivisione risulterebbe preimpostato ¹²⁷. Tanto più che, come rileva l'AGCM, Facebook prospetta in conseguenza della disattivazione della condivisione conseguenze penalizzanti per l'utente nella fruizione, nella accessibilità e nell'utilizzo della piattaforma ¹²⁸. In questo caso l'AGCM sanziona comportamenti che hanno grande rilievo per la disciplina *data protection*, ed infatti erano state evidenziate dal WP29, e che ben potrebbero essere oggetto di analisi da parte delle preposte Autorità di Controllo. Ed infatti, sinteticamente, la pratica di preimpostare il consenso dell'utente è radicalmente vietata dal GDPR. Un consenso preimpostato o presunto non è infatti considerato valido e ciò produce l'illiceità dell'intero trattamento. Inoltre, altri aspetti meriterebbero di essere analizzati alla luce del GDPR. Per esempio, la pratica di preimpostare il servizio nel modo più invasivo per la privacy, ossia al fine di raccogliere quanti più dati possibili, sembrerebbe porsi in modo diametralmente opposto rispetto a quanto previsto dai principi di *privacy by design* e *by default* ex art. 25 GDPR. Così come sarebbe interessante verificare che tipo di analisi ha condotto Facebook nell'ambito della "valutazione d'impatto sulla protezione dei dati" (c.d. DPIA) ex art. 35 e ss GDPR con riferimento a servizi quali la profilazione ma anche alla pratica della condivisione dei dati con ogni soggetto terzo.

A tal proposito, auspicando l'intervento anche delle Autorità di controllo in materia di protezione dei dati personali, si rileva qui uno stretto legame tra gli istituti a tutela del consumatore/interes-

¹²⁵ Provvedimento AGCM PS11112, *cit.*, punto 4 e 55 e ss e 70.

¹²⁶ L'AGCM rileva come il business model del gruppo Facebook si basi « sulla raccolta e sfruttamento dei dati degli utenti a fini remunerativi configurandosi, pertanto, tali dati come contro-prestazione del servizio offerto dal social network, in quanto dotati di valore commerciale. In particolare, i ricavi provenienti dalla pubblicità on

line, basata sulla profilazione degli utenti a partire dai loro dati, costituiscono l'intero fatturato di Facebook Ireland Ltd. e il 98% del fatturato di Facebook Inc ». Provvedimento AGCM PS11112, *cit.*, punto 18. Si veda anche il punto 54.

¹²⁷ Provvedimento AGCM PS11112, *cit.*, punti 26 ss.

¹²⁸ Provvedimento AGCM PS11112, *cit.*, punti 5 e 23 e 57 e ss e 71.

sato, in relazione al trattamento dei loro dati personali, che ben concretizza l'applicazione convergente delle norme coinvolte. È infatti evidente come le fattispecie evidenziate abbiano rilevanza per entrambe le normative ¹²⁹.

In ambito europeo altre Autorità si sono poi occupate del tema, confermando la rilevanza del caso sia per la normativa *data protection*, sia per quella sulla concorrenza che per la tutela del consumatore, e alimentando questo “dialogo” a distanza tra Autorità. Tra queste, in particolare si rileva il Bundeskartellamt, l'Autorità tedesca sulla concorrenza, che ha contestato a Facebook un abuso di posizione dominante sul mercato tedesco dei *social network* tramite la possibilità di accumulare senza limiti tutti i tipi di dati generati dall'uso di servizi terzi ma di sua proprietà come WhatsApp o Instagram, e tramite siti Web e app di altri operatori con API (*Application Programming Interfaces*) di Facebook incorporate ¹³⁰.

Anche l'*Information Commissioner's Office* inglese ha dichiarato illecita la condivisione di dati tra WhatsApp e Facebook. Con questa Autorità, WhatsApp si è impegnata a conformare la condivisione di questi dati secondo le regole del Regolamento UE 2016/679 e secondo le indicazioni della Autorità di controllo Irlandese in qualità di Autorità capofila ¹³¹.

6. RIMEDI EX ANTE AVVERSO TRATTAMENTI ABUSIVI DEI DATI: GLI ARTT. 20 E 25 GDPR.

Di particolare interesse con riferimento all'uso abusivo dei dati già raccolti e poi elaborati in ulteriori mercati per finalità ulteriori sono quei rimedi che rientrano nel concetto di *privacy—enhancing services* ¹³². Con tale etichetta si fa riferimento a tutte quelle tecnologie, tecniche e servizi che tutelano la privacy delle persone limitando, riducendo, eliminando o impedendo di racco-

¹²⁹ Cfr. Provvedimento AGCM PS11112, *cit.*, punti 45 e 46 in cui si rileva che: « non sussiste un conflitto di tra le due discipline, integrandosi, piuttosto, le stesse in maniera complementare ». Si veda anche il punto 47.

¹³⁰ Bundeskartellamt, *Preliminary assessment in Facebook proceeding: Facebook's collection and use of data from third-party sources is abusive*, 19 December 2017, press release disponibile al link: www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html. Cfr. ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, *cit.*, p. 259 ss. Si vedano anche: A. MASSOLO, *Bundeskartellamt vs Facebook: time to refresh “GDPR's wall”?*, in *Italian Antitrust Review*, n. 1 (2018), p. 77- 84; G. COLANGELO, M. MAGGIOLINO, *Big data, Protection and Antitrust in the wake of the Bundeskartellamt case against Facebook*, in *Italian Antitrust Review*, n. 1, 2017, p. 104-112.

¹³¹ Information Commissioner's Office, *WhatsApp Inc. has signed an undertaking with the Information Commissioner*, 14 March 2018, disponibile al link: <https://ico.org.uk/action-weve-taken/enforcement/whatsapp-inc/>.

¹³² Commissione Europea, COM (2007) 228, *cit.*; si veda anche R. D'ORAZIO, *Protezione dei dati by default e by design*, in S. SICA, V. D'ANTONIO, G. M. RICCIO (a cura di), *La nuova disciplina della privacy*, Padova, 2016, p. 99 ss.

gliere ed elaborare quei dati non necessari al trattamento ad oggetto. L'importanza e l'interesse per tali sistemi è evidente nella misura in cui vengono a creare dei rimedi *ex ante*, a monte del trattamento, nella c.d. fase zero, impedendo o limitando le possibilità di usi distorti e rischiosi dei dati personali.

In questa categoria rientrano istituti come la minimizzazione dei dati¹³³ ma anche la limitazione del tempo di conservazione¹³⁴.

Particolare attenzione la destano gli istituti della "protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" di cui all'art. 25 GDPR¹³⁵ e il diritto alla portabilità dei dati di cui all'art. 20 GDPR.

Con riferimento ai primi, l'art. 25 comma 1 GDPR dispone che il titolare del trattamento metta in atto misure tecniche e organizzative adeguate per attuare in modo efficace i principi di protezione dei dati quali la minimizzazione. Il concetto a cui la norma fa riferimento è comunemente conosciuto come *data protection by design*¹³⁶.

Il secondo comma del medesimo art. 25 impone invece al titolare del trattamento di adottare misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. È questo il c.d. principio della *data protection by default* che impone al titolare di impostare il trattamento in modo da raccogliere solo i dati pertinenti e limitati a quanto necessario per le finalità del trattamento (principio di minimizzazione)¹³⁷. È questa una previsione di utilità strategica nella misura in cui tiene conto dell'inerzia dell'interessato nella gestione delle impostazioni che il servizio prevede per il trattamento dei dati personali. La norma sembrerebbe quasi far proprie le teorie dell'economia comportamentale sul *nudge* e in ottica proattiva porre rimedio a quell'inconsapevole inerzia dell'interessato che potrebbe arrecargli danno¹³⁸. In questo caso ci troviamo, infatti, in una fase in cui

¹³³ FRA - CoE - ECHR - EDPS, *Handbook on European data protection law*, cit., p. 125 e ss.; L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 84 ss.

¹³⁴ FRA - CoE - ECHR - EDPS, *Handbook on European data protection law*, cit., p. 129 e ss.; L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 110; con riferimento al principio di minimizzazione, alla *data retention*, ma in generale al principio di precauzione, si veda R. D'ORAZIO, *Protezione dei dati by default e by design*, cit., p. 85 e ss e 105 ss.

¹³⁵ R. D'ORAZIO, *Protezione dei dati by default e by design*, cit., p. 79 e ss.; Si veda anche L. JASMONTAITE, I. KAMARA, G.

ZANFIR-FORTUNA, S. LEUCCI, *Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR*, in *European Data Protection Law Review*, No. 2, 06.2018, p. 168-189.

¹³⁶ Cfr. European Data Protection Supervisor, *Opinion 5/2018: Preliminary Opinion on privacy by design*, 31 May 2018, disponibile al link: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

¹³⁷ R. D'ORAZIO, *Protezione dei dati by default e by design*, cit., p. 80 ss.

¹³⁸ Secondo Richard Thaler e Cass Sunstein il *nudge* è « ogni aspetto nell'architettura delle scelte che altera il compor-

il trattamento dei dati è iniziato e può proseguire secondo diverse modalità. La norma, col riferimento al concetto di *data protection by default*, stabilisce che in assenza di alcun intervento o scelta da parte dell'interessato il trattamento deve svolgersi in automatico secondo le modalità meno invasive della sfera privata dell'interessato e quindi in modo tale da raccogliere meno dati possibile.

Tali principi, prima rintracciabili *in nuce* nel principio di necessità¹³⁹ di cui all'art. 3 della versione originaria del d.lgs. 196/2003¹⁴⁰ con riferimento esclusivo ai sistemi informativi e i programmi informatici, possono essere considerati già impliciti nei principi di limitazione della finalità e di minimizzazione. Il riconoscimento degli stessi, in modo esplicito, nell'art. 25 GDPR ne sottolinea l'importanza creando un'autonoma prescrizione all'adozione di misure tecniche che vadano incontro all'interesse degli utenti a che i loro dati non siano trattati per scopi diversi rispetto a quelli per i quali erano stati prestati. In altre parole, il ricorso a tali istituti con riferimento alla fattispecie di uso secondario di dati aiuta a tutelare le legittime aspettative degli interessati su come vengono trattati i propri dati evitando, "*per impostazione predefinita*" appunto, il loro uso per altre finalità¹⁴¹.

Queste due norme, ancorché non idonee a impedire del tutto o porre rimedio ad un uso ulteriore dei dati personali non compatibile, possono comunque operare come limite al rischio di trattamenti scorretti riducendo il numero di dati a disposizione del titolare e contestualmente aumentando il livello di tutela dell'interessato.

L'art. 20 GDPR prevede invece il diritto alla portabilità dei dati¹⁴², per tale intendendosi il diritto dell'interessato di ricevere i dati personali che lo riguardano e da lui "forniti a" un titolare del trattamento, « in un formato strutturato, di uso comune e

tamento delle persone in modo prevedibile senza proibire la scelta di altre opzioni e senza cambiare in maniera significativa i loro incentivi economici ». Sarebbe quindi un incentivo per spingere naturalmente il soggetto a compiere una decisione per lui benefica ma che altrimenti non avrebbe preso. La teoria, contenuta nel libro R. THALER - C. SUSTEIN, *Nudge: La spinta gentile*, Milano, 2009, ha permesso a Thaler di vincere nel 2017 il premio Nobel per l'economia.

¹³⁹ L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 106.

¹⁴⁰ Prima delle modifiche apportate dal d.lgs. 101/2018, l'art. 3 del d.lgs. 196/2003 recitava: « Principio di necessità nel trattamento dei dati - I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati

personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità ».

¹⁴¹ EDPS, *Opinion 5/2018: Preliminary Opinion on privacy by design*, cit., p. 7.

¹⁴² Sul diritto alla portabilità dei dati si vedano anche: FRA - CoE - ECHR - EDPS, *Handbook on European data protection law*, cit., p. 228 e ss.; P. PACILEO, *Il diritto alla portabilità*, in S. SICA, V. D'ANTONIO, G. M. RICCIO (a cura di), *La nuova disciplina della privacy*, Padova, 2016, p. 221-240; L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 246 ss.

leggibile da dispositivo automatico », e conseguentemente il diritto di trasmettere tali dati a un altro titolare del trattamento, anche direttamente dal vecchio al nuovo titolare ¹⁴³.

Anche se nata nel contesto della protezione dei dati personali, tale norma può rivestire una valenza antitrust contro fenomeni di *lock-in* essendo potenzialmente idonea a promuovere la concorrenza tra operatori in relazione alla gestione dei dati personali.

Con riferimento al caso di uso secondario di dati oggetto della presente indagine, questa norma più che una valenza inibitoria ha lo scopo di riequilibrare le posizioni di forza tra i soggetti coinvolti, permettendo all'interessato di spostare i propri dati ad un altro titolare del trattamento esplicitando quindi l'intenzione di ricevere un certo servizio, in via esclusiva o anche cumulativa, da parte di un altro titolare del trattamento.

In questo modo, il diritto alla portabilità dei dati permetterebbe di promuovere la concorrenza, abbassando le barriere all'entrata per i nuovi operatori e spingendo gli operatori già presenti sul mercato a implementare e migliorare i propri servizi ¹⁴⁴ nonché riducendo i cc.dd. *switching cost* per il consumatore/utente, ossia gli ostacoli di diversa natura che rendono difficile o impediscono di passare da un servizio facilitandolo così nella gestione dei propri dati ¹⁴⁵. Potrebbero quindi essere gli stessi utenti a decidere a quale operatore fornire i propri dati, determinando uno spostamento di risorse fondamentali per l'economia *data driven*. Allo stesso tempo, la norma dovrebbe spingere gli stessi operatori a competere per invogliare gli utenti a mantenere presso di loro i dati o a spostarli e riceverli da un operatore all'altro ¹⁴⁶.

Così facendo, il diritto alla portabilità dei dati potrebbe porsi come strumento di prevenzione di fenomeni di abuso di posizione dominante che sfruttino il fatto che i consumatori si trovino bloccati in determinati servizi a causa di condizionamenti tecnologici o di altra natura. Inoltre, la portabilità dei dati potrebbe consentire ai consumatori di usufruire dei servizi a valore aggiunto di imprese terze facilitando l'accesso al mercato da parte di concorrenti, aumentando la scelta del consumatore e tutelando la concorrenza ¹⁴⁷. Ciò sarà tendenzialmente vero soprattutto se tale diritto viene usato nei confronti di grandi operatori in posizione di

¹⁴³ Cfr. Gruppo di lavoro Articolo 29, *Linee-guida sul diritto alla "portabilità dei dati"*, WP 242 rev.01, Adottate il 13 dicembre 2016 - Versione emendata e adottata il 5 aprile 2017, disponibili al link: <https://stepnews.isti.cnr.it/wp-content/uploads/2017/12/Linee-guida-sul-diritto-alla-portabilit%C3%A0-dei-dati-WP-242.pdf>.

¹⁴⁴ G. PITRUZZELLA, *Big Data, Competition and Privacy*, cit., p. 26.

¹⁴⁵ W. KERBER, *Digital markets, data,*

and privacy: competition law, consumer law and data protection, cit., p. 10; ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 282 ss.

¹⁴⁶ ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 258 e 317 ss.

¹⁴⁷ EDPS, *Privacy and competitiveness in the age of big data*, cit., § 83.

dominanza. Diversamente, potrebbe presentare aspetti di criticità se usato nei confronti di nuovi operatori e *start up*. In questi casi, infatti, non si è mancato di evidenziare come l'applicabilità indifferenziata dal diritto alla portabilità dei dati a tutte le imprese potrebbe costituire un costo eccessivo per *start up* e piccoli operatori tale da comprometterne la competitività riducendone il profitto e gli incentivi a innovare¹⁴⁸.

In concreto quindi, se l'impresa X decidesse di usare i dati in suo possesso per offrire un servizio Y potrebbe scontrarsi contro lo sfavore dell'utente. Così facendo i suoi profitti e quote di mercato potrebbero essere ridotti dalla scelta dell'interessato di preferire comunque di ricevere il servizio da un'impresa già operante nel mercato o da una nuova *start up* che possa sembrare agli occhi dell'utente più innovativa, aiutandola così ad affermarsi sul mercato. Potrebbe essere un'ipotesi poco applicata ma, in astratto, possibile, come possibile potrebbe essere il fenomeno opposto, ossia che la portabilità dei dati si rilevi uno strumento a vantaggio dell'operatore OTT che entra in un nuovo mercato o decida di offrire un nuovo servizio.

Ciononostante, è indubbio come la portabilità dei dati ben potrebbe contribuirebbe a ridurre ed attenuare gli squilibri tra i soggetti coinvolti, permettendo agli interessati di gestire la "ricchezza" creata dai loro dati e, d'altra parte, incentivare gli sviluppatori a offrire ulteriori servizi che si basino proprio su dati portabili¹⁴⁹.

Infine, sono stati prospettati ulteriori rimedi *ex ante* avverso l'uso secondario non corretto di big data. Rimedi però ancora oggetto di valutazione in quanto alcuni rischierebbero di essere rigettati dal mercato e comunque applicabili in presenza di determinate condizioni e salvaguardie¹⁵⁰.

Tra questi: sulla base della già accennata concezione del dato come *essential facility*, l'obbligo per una società in posizione dominante di cedere copia dei propri *data base* o consentirne l'accesso; reintrodurre l'offerta di servizi a pagamento al fine di ridurre al minimo la necessità della raccolta e la conservazione di dati; individuare dei limiti proporzionali per la conservazione dei dati; implementare e incentivare la portabilità dei dati; porre in

¹⁴⁸ Cfr. G. MUSCOLO, *Big data e concorrenza. Quale rapporto?*, cit., p. 184; P. SWIRE - Y. LAGOS, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 Md. L. Rev. 335, 2013, disponibile al link: <http://digitalcommons.law.umaryland.edu/mlr/vol72/iss2/1/>; ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 285.

¹⁴⁹ Gruppo di lavoro Articolo 29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della Direttiva 95/46/CE*, cit., p. 56 ss.

¹⁵⁰ Come rileva F. DI PORTO, *La rivoluzione big data*, cit., p. 6, le nuove e in larga parte inesprese potenzialità dei big data suggeriscono prudenza e l'adozione di approcci non eccessivamente interventisti.

essere controlli rigorosi e un'interpretazione restrittiva del concetto di "compatibilità" del trattamento ulteriore con quello originario ¹⁵¹.

Inoltre, particolare interesse lo desta la c.d. separazione funzionale dei dati, ossia una misura organizzativa diretta a inibire l'utilizzo di alcune categorie di dati per svolgere certe attività d'impresa ¹⁵². Ad esempio e dando attuazione anche al già visto art. 6 paragrafo 4 GDPR, il diritto dell'Unione o degli Stati Membri potrebbe, ex art. 23 GDPR, limitare o regolare il trattamento di categorie particolari di dati per tutelare l'interessato o i diritti e le libertà altrui (art. 23, par. 1, lett. i).

Su questa scia si prospettano diverse soluzioni in teoria possibili ma che necessiterebbero comunque di un'accurata valutazione di impatto prima di una loro applicazione pratica e concreta.

In questo senso, una possibilità potrebbe essere vietare che categorie particolari di dati, per esempio l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati relativi alla salute o all'orientamento sessuale della persona, siano usati per attività di *business*, *marketing* o utilizzo ulteriore e secondario. Questo al fine di evitare i rischi connessi non solo all'utilizzo secondario di big data ma anche fenomeni quali le *fake news* o l'alterazione e il condizionamento dell'opinione pubblica nei processi democratici quali l'esercizio del diritto di voto.

Altra soluzione astrattamente possibile potrebbe essere determinare *ex lege* le basi giuridiche sulle quali possono avvenire particolari tipi di trattamento secondario di dati, escludendo quelle basi ritenute non idonee, per esempio il consenso o il contratto. Un esempio di tal specie è rinvenibile nell'art. 9 GDPR laddove, diversamente dell'art. 6, si esclude che il trattamento di categorie particolari di dati avvenga sulla base di un contratto o dell'interesse legittimo e, oltre a fornire basi di liceità specifiche, rafforza il requisito del consenso prevenendo un "consenso esplicito" ¹⁵³.

¹⁵¹ EDPS, *Privacy and competitiveness in the age of big data*, cit., § 72.

¹⁵² Gruppo di lavoro Articolo 29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della Direttiva 95/46/CE*, cit., p. 50, che identifica col concetto di separazione funzionale tutte quelle misure tecniche e organizzative volte a garantire che i dati non siano utilizzati per adottare decisioni o intraprendere altre azioni riguardo alle persone. Nell'*Opinion 03/2013 on purpose limitation*, cit., p. 30, si ritiene che « The notion of "functional separation" means that data used for statistical purposes or other research purposes should not be available to "support measures or decisions" that are taken with regard to the individual data subjects concerned ». Si veda anche L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 102.

¹⁵³ Sull'istituto del consenso esplicito si vedano: C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, cit., p. 115 e ss.; FRA - CoE - ECHR - EDPS, *Handbook on European data protection law*, cit., p.

Allo stesso modo, si potrebbe prevedere che l'uso secondario di dati si basi sul consenso esplicito, su specifiche ipotesi predeterminate dalla legge e non altre, e che tratti solo alcune categorie di dati, rendendo quindi illecito il trattamento al di fuori di queste condizioni, con conseguente inutilizzabilità dei dati raccolti e sanzionabilità dell'impresa. Un esempio significativo in tal senso è oggi rinvenibile nella normativa sui servizi di pagamento dove, il ricorso ai servizi di disposizione di ordine di pagamento e di informazione sui conti è ammesso solo previo "consenso esplicito" e in presenza di alcune misure che tutelino i dati coinvolti da usi ulteriori non autorizzati ¹⁵⁴.

7. IL DIRITTO DI OPPOSIZIONE.

Con riferimento, infine, a quei rimedi che più che prevenire permettono di porre rimedio all'uso incompatibile dei dati con lo scopo originario, ci si limiterà ad accennare al diritto di opposizione come contraltare dell'utilizzo, da parte del titolare, del legittimo interesse (*legitimate interest*) come base giuridica del trattamento secondario ¹⁵⁵.

Il diritto di opposizione di cui all'art. 21 GDPR assume infatti importanza in tutti quei casi in cui, non essendo il consenso la base giuridica del trattamento, l'interessato non potrebbe esercitare il diritto di revoca ex art. 7, paragrafo 3, GDPR ¹⁵⁶.

È inoltre, come esplicitamente riconosciuto dai paragrafi 2 e 3 GDPR, un diritto importante soprattutto quando l'ulteriore trattamento dei dati sia fatto per finalità di marketing ¹⁵⁷.

Il Considerando 47 ammette che: « Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto ». Se tale considerando potrebbe legittimare l'utilizzo dei

161; L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 223 ss.

¹⁵⁴ Cfr. artt. 66 e 67 Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno (c.d. PSD2).

¹⁵⁵ Per un'analisi più approfondita del diritto di opposizione si veda: FRA - CoE - ECHR - EDPS, *Handbook on European data protection law*, cit., p. 229 ss.; P. PACILEO, *Profilazione e diritto di opposizione*, in S. SICA, V. D'ANTONIO, G. M. RICCIO (a cura di), *La nuova disciplina della privacy*, Padova, 2016, p. 177-196; L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 239 ss.

¹⁵⁶ « Il [titolare] del trattamento può trattare i dati, subordinatamente a determinate condizioni e garanzie, purché l'interes-

sato non si sia opposto. In questo senso, il diritto di opposizione può piuttosto essere considerato come una forma specifica di revoca del consenso ». Così Gruppo di lavoro Articolo 29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della Direttiva 95/46/CE*, cit. p. 54.

¹⁵⁷ F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit., p. 31 e ss.; O. SESSO SARTI, *Profilazione e trattamento dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, p. 600; FRA - CoE - ECHR - EDPS, *Handbook on European data protection law*, cit., p. 231; P. PACILEO, *Profilazione e diritto di opposizione*, cit., p. 190 ss.

dati per finalità di marketing senza il consenso dell'interessato, allo stesso tempo il GDPR vede nel diritto di opposizione il contrappeso a tutela dell'interessato¹⁵⁸. L'art. 21, paragrafi 2 e 3 prevedono infatti che: « [2] Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. [3] Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità ».

Infine nulla vieta e, anzi, potrebbe essere auspicabile che il titolare del trattamento che intenda basare l'utilizzo ulteriore dei dati in suo possesso sul legittimo interesse riconoscesse all'interessato, pur non essendone tenuto, anche un autonomo diritto di revoca come ulteriore garanzia supplementare. La revoca infatti permetterebbe di ottenere la cessazione del trattamento senza che l'interessato sia tenuto a dimostrare alcunché¹⁵⁹. Diversamente il diritto di opposizione, pur essendo lo specifico strumento che garantisce dai trattamenti che si basano sul legittimo interesse o su compiti di interesse pubblico o connessi all'esercizio di pubblici poteri, è subordinato alla dimostrazione di motivi particolari connessi alla situazione dell'interessato (art. 21 GDPR).

Tale possibilità acquisirà importanza soprattutto in quei casi limite in cui il bilanciamento degli interessi di titolare e interessato per ricorrere all'interesse legittimo dovesse risultare particolarmente problematico. In questi casi il riconoscimento della revoca come ulteriore strumento, pur non essendo collegata all'istituto del consenso, integrerebbe una garanzia per l'interessato. L'utilità per l'interessato risiederebbe nella possibilità di usufruire di uno strumento più agevole per ottenere la cessazione del trattamento, ma anche il titolare se ne avvantaggerebbe perché grazie a questa previsione potrebbe più facilmente ottenere il riconoscimento della legittimità del ricorso all'interesse legittimo facendo

¹⁵⁸ « Il diritto di opposizione è invece assoluto, e comporta l'interruzione immediata e definitiva dei trattamenti, quando i dati siano trattati per finalità di marketing diretto nell'ambito di una lettura dell'interesse legittimo del titolare che si estenda anche a questa finalità, compresa eventualmente la profilazione ». Così F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit., p. 32.

¹⁵⁹ Gruppo di lavoro Articolo 29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della Direttiva 95/46 CE*, cit., p. 53: « Il Gruppo di lavoro sottolinea che, sebbene il diritto di opposizione di cui all'articolo 14, lettera a), debba essere giustificato dall'interessato, nulla vieta al responsabile del trattamento di offrire la possibilità di revocare il consenso che, oltre a costituire un'opzione più ampia, non comporterebbe la necessità di fornire una dimostrazione supplementare dell'interesse legittimo da parte dell'interessato ».

timo del responsabile del trattamento ai sensi dell'articolo 7 della Direttiva 95/46 CE, cit., p. 53: « Il Gruppo di lavoro sottolinea che, sebbene il diritto di opposizione di cui all'articolo 14, lettera a), debba essere giustificato dall'interessato, nulla vieta al responsabile del trattamento di offrire la possibilità di revocare il consenso che, oltre a costituire un'opzione più ampia, non comporterebbe la necessità di fornire una dimostrazione supplementare dell'interesse legittimo da parte dell'interessato ».

pendere a suo favore gli esiti del test comparativo richiesto dal GDPR¹⁶⁰.

In questo modo, un meccanismo di revoca adeguatamente strutturato ed efficace potrebbe svolgere un ruolo importante nella salvaguardia dei diritti e degli interessi delle persone fisiche e interessati, che risultino coinvolti nell'uso secondario dei dati.

8. CONCLUSIONI.

All'esito di tale trattazione si è tentato di evidenziare come una convergenza tra le normative in materia di *data protection* e *competition* possa portare benefici reciproci per raggiungere il fine comune della fiducia nei mercati. In particolare si è visto come istituti e principi contenuti nel Regolamento UE 2016/679 possano rivestire una valenza nelle analisi antitrust. Infatti, il principio di limitazione delle finalità, il cui scopo principale è quello di vietare usi alternativi dei dati personali non compatibili con le finalità originarie del trattamento, può essere utile per individuare attività distorsive della concorrenza tramite il riutilizzo dei dati o il loro uso secondario e nel passaggio da un mercato all'altro¹⁶¹. Infine, può essere un indizio, una figura sintomatica che, senza creare alcun automatismo¹⁶², possa essere tenuta in considerazione nei procedimenti per abuso di posizione dominante¹⁶³ o nelle valutazioni relative alle operazioni di concentrazioni¹⁶⁴ tra multinazionali e piattaforme digitali. Questo contribuendo anche allo sviluppo o la semplice implementazione di una "*theory of harm*" insieme ad altri fattori tipici di un'analisi antitrust¹⁶⁵.

¹⁶⁰ « Quanto più ampiamente applicabile sarà il meccanismo di revoca del consenso e quanto più semplice sarà esercitarlo, tanto più tale meccanismo contribuirà a far pendere il bilanciamento a favore del trattamento ». Così Gruppo di lavoro Articolo 29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della Direttiva 95/46/CE*, cit., p. 53 ss.

¹⁶¹ « In the context of the digital economy, it is therefore feasible that a company can be able to collect data to act on such market and then process the same data to compete in a different market. Data compatibility thus can change all the analysis of a market and its configuration, to determine the dominant position and market power of an entrepreneur and the existence of barriers to entry ». Così V. BAGNOLI, *The big data relevant market*, cit., p. 79.

¹⁶² ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di*

mercato e prospettive di policy, cit., p. 260 ss.

¹⁶³ W. KERBER, *Digital markets, data, and privacy: competition law, consumer law and data protection*, cit., p. 10 ss.

¹⁶⁴ G. PITRUZZELLA, *Big data and anti-trust enforcement*, cit., p. 81 e ss.; G. MUSCOLO, *Big data e concorrenza. Quale rapporto?*, cit., p. 181 e ss, la quale, sottolineando l'importanza delle operazioni dirette all'acquisizione di dati, riconosce come rilevate nel controllo delle concentrazioni anche il ruolo delle *privacy policy* come parametro di concorrenza non fondata sul prezzo (*no price dimension*); ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 221 ss.

¹⁶⁵ « This theory of harm needs to be assessed in light of a number of specific factors: (i) the scope of the relevant downstream product market; (ii) market structure; (iii) the importance of data for the

Un esempio semplice ma efficace della rilevanza e utilità della convergenza con la disciplina *data protection* è rinvenibile, oltre ai casi già visti, anche in riferimento ad altri settori quali la regolazione nell'ambito delle comunicazioni elettroniche di competenza dell'Autorità per le Garanzie delle Comunicazioni. In proposito, e a riprova di quanto sopra, si prenda come esempio un ulteriore caso di “dialogo” tra Autorità amministrative indipendenti con riferimento alla vicenda della società Supermoney S.p.A., svolgente attività di comparatore di prezzi in qualità di motore di calcolo ¹⁶⁶. Nello specifico, in seguito ad accertamenti, il Garante per la Protezione dei Dati Personali ha rilevato come tale società raccogliesse dati personali in modo illecito e, in conseguenza di ciò, ne ha vietato il trattamento ¹⁶⁷. Due mesi dopo, tale provvedimento è stato seguito da quello dell'Autorità per le Garanzie nelle Comunicazioni che, prendendo atto della violazione accertata del Garante e ritenendo il mancato rispetto della normativa *data protection* rilevante per il settore dei motori di calcolo di sua competenza, ha deliberato la decadenza dell'accreditamento del motore di calcolo Supermoney per la comparazione dei prezzi dei servizi di comunicazione elettronica ¹⁶⁸. È questo un esempio, forse banale, che ben evidenzia come la disciplina e gli strumenti in materia di *data protection* possano rivestire importanza e nuova utilità come ulteriori elementi di valutazione nell'ambito di altre normative.

Tornando al tema centrale della presente trattazione, la disciplina sulla concorrenza potrebbe non essere sempre sufficiente ad un'analisi completa delle attività e dei servizi basati sulla gestione di big data. In questi casi una normativa *data protection* chiara

supply of the downstream service; (iv) rivals' capabilities to collect similar information; (v) the existence of third party sources through which substitutable information can be collected ». Così G. PITRUZZELLA, *Big Data, Competition and Privacy*, cit., p. 20; ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 258 ss.

¹⁶⁶ Un motore di calcolo è un programma informatico che permette il confronto tariffario tra le diverse offerte degli operatori. Tali motori di calcolo devono soddisfare particolari requisiti di trasparenza, correttezza ed indipendenza dei relativi siti web. Cfr. AgCom, *Motori di calcolo per la comparazione tariffaria*: www.agcom.it/motori-di-calcolo-per-la-comparazione-tariffaria.

¹⁶⁷ Il Garante per la protezione dei dati personali ha accertato come la società Supermoney si avvallesse di un pop-up per raccogliere il consenso al trattamento dei

dati personali. Tuttavia questo non permetteva di esprimere consensi specifici e separati. Non si dava quindi all'interessato la possibilità di accedere ai servizi offerti senza accettare il trattamento dei dati personali per tutte le finalità, comprese quelle di marketing o comunicazione dei dati a terzi. Provvedimento del Garante per la Protezione dei Dati Personali n. 363 del 22 maggio 2018, doc. web n. 8995274, *Trattamento dei dati raccolti attraverso pop up*, disponibile al link: www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8995274.

¹⁶⁸ Delibera dell'Autorità per le Garanzie nelle Comunicazioni n. 391/18/CONS del 25 luglio 2018, *Decadenza dell'accreditamento del motore di calcolo “Supermoney.eu” di cui alla delibera n. 22/10/CONS*, disponibile al link: www.agcom.it/documents/10179/11192137/Delibera+391-18-CONS/8ec71e58-900d-4062-93adb817f8e514f?version=1.0.

e adeguata potrebbe anche operare come ulteriore elemento di ausilio nell'analisi del servizio e nella valutazione della dimensione del processo competitivo ¹⁶⁹. Infatti, il rispetto della privacy e il corretto trattamento dei dati è oggi un elemento importante di fiducia nei servizi digitali, necessario affinché i mercati on line funzionino senza problemi e siano motore di crescita e competitività ¹⁷⁰.

Una convergenza tra le due discipline sarà quindi naturale nella misura in cui la gestione dei big data, specie con riferimento ad imprese in posizione di dominanza ¹⁷¹, crea ambiti di sovrapposizione tra privacy e concorrenza. Tale convergenza dovrebbe inoltre essere perseguita nella misura in cui sia utile a rafforzare la tutela dei dati personali e rimuovere le corrispondenti criticità dal punto di vista concorrenziale ¹⁷².

Chiaramente non tutte le problematiche in materia di *data protection* connesse ai big data saranno automaticamente rilevanti in ambito antitrust e viceversa ma laddove non può arrivare l'una potrebbe arrivare l'altra e la conoscenza di una normativa può essere fonte di elementi utili per l'analisi svolta dell'altra ¹⁷³. D'altronde, entrambe le materie hanno la stessa *ratio*: raggiungere e preservare la fiducia nel mercato.

Tuttavia, per una corretta valutazione degli effetti e della portata del principio di limitazione delle finalità occorrerà ancora attendere. Bisognerà infatti vedere come questo istituto vivrà nelle maglie della complessa regolazione di Internet ¹⁷⁴ e come sarà applicato tanto dalle Autorità di controllo per la protezione dei dati personali, quanto, eventualmente, dalle *competition au-*

¹⁶⁹ « Ultimately, it would be desirable to have markets in which privacy becomes a key dimension of consumers' perceived service quality and therefore a dimension of the competitive process ». Così G. PITRUZZELLA, *Big Data, Competition and Privacy*, cit., p. 26.

¹⁷⁰ G. PITRUZZELLA, *Big Data, Competition and Privacy*, cit., p. 26 ss.

¹⁷¹ A tal riguardo, secondo le autorità per la concorrenza francese e tedesca: « privacy policies could be considered from a competition standpoint whenever these policies are liable to affect competition, notably when they are implemented by a dominant undertaking for which Data serves as a main input of its products or services ». AUTORITÉ DE LA CONCURRENCE (FR) - BUNDESKARTELLAMT (DE), *Competition Law and Data*, cit., p. 23-24.

¹⁷² Cfr. W. KERBER, *Digital markets, data, and privacy: competition law, consumer law and data protection*, cit., p. 19.

¹⁷³ Cfr. G. PITRUZZELLA, *Big Data, Competition and Privacy*, cit., p. 15.

¹⁷⁴ Sugli aspetti giuridici di Internet si vedano: V. ZENO-ZENCOVICH, *Data protection in the Internet*, in *Annuario di diritto comparato e di studi legislativi*, 2018, p. 431-439; M.R. ALLEGRI, *Ubi Social, Ibi Ius. Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei provider*, Milano, 2018; T.E. FROSINI, *Internet e democrazia*, in *Diritto dell'informazione e dell'informatica*, fasc. 4-5, 2017, p. 657-671; T.E. FROSINI, O. POLLICINO, E. APA, M. BASINI (a cura di), *Diritti e libertà in Internet*, Milano, 2017; O. POLLICINO, G. ROMEO, *The Internet and Constitutional Law: The protection of fundamental rights and constitutional adjudication in Europe*, Routledge Research in Constitutional Law, 2016; F. MARCELLI, P. MARSOCCI, M. PIETRANGELO, *La rete internet come spazio di partecipazione politica. Una prospettiva giuridica*, Napoli, 2015; T.E. FROSINI, *Libertà, egualità, internet*, Napoli, 2015; M. NISTICÒ, P. PASSAGLIA (a cura di), *Internet e Costituzione*, Torino, 2014; O. POLLICINO, E. BERTOLINI, V. LUBELLO (a cura di), *Internet: regole e tutela dei*

thorities nazionali e europea. Ciò è tanto più necessario laddove la portata del principio necessita ancora di chiarimenti. Non mancano infatti valutazioni critiche espresse dalla dottrina. In tal senso, Pizzetti ravvisa nella lettera dell'art. 5 GDPR, con riferimento al principio di limitazione della finalità, una « *formula quanto meno ambigua, che fa ritenere che i trattamenti possano avvenire sulla base di una lettura molto ampia delle finalità per le quali sono stati raccolti, visto che il solo limite è la "non incompatibilità"* ». Tale considerazione sarebbe supportata dal fatto che l'art. 6 paragrafo 4 allargherebbe di molto le possibilità di trattare i dati per finalità diverse da quelle originarie ¹⁷⁵. Dello stesso avviso — seppur con riferimento al contesto della Direttiva 95/46/CE e, quindi, a un atto che, contrariamente al regolamento, mirando ad una armonizzazione e non anche all'uniformazione della normativa nei vari Stati membri, per sua natura va incontro al rischio di un'applicazione differenziata — era il Gruppo di lavoro articolo 29 secondo il quale la formulazione del principio di limitazione della finalità risulta molto aperta e perciò suscettibile di interpretazioni diverse ¹⁷⁶. A chiosa di tali opinioni, Colapietro e Iannuzzi rilevano come tale principio si presti ad un'elasticità interpretativa che, se da una parte conferisce flessibilità al sistema, dall'altra ne vincola l'analisi ad una valutazione secondo un approccio *case by case*, tenendo conto quindi della concretezza della situazione di fatto di volta in volta rilevante ¹⁷⁷. Valutazione questa che dovrebbe essere svolta con maggiore attenzione e precisione nel momento in cui si adottino tecnologie e sistemi per il trattamento dei big data ¹⁷⁸.

Dunque, nonostante lo sforzo di una trattazione generale del tema, il corretto inquadramento dei principi di *data protection* nell'ambito di un sistema di *competition law* non potrà prescindere da una valutazione caso per caso delle questioni di volta in volta rilevanti ¹⁷⁹. La singola questione andrà quindi esaminata secondo un "*case by case approach*", individuando il mercato di

diritti fondamentali, Roma, 2013; G. DE MINICO, *Internet. Regola e anarchia*, Napoli, 2012; G. AZZARITI, *Internet e Costituzione*, in *Politica del diritto*, n. 3, 2011, p. 367-378; S. SICA, V. ZENO-ZENCOVICH, *Legislazione, giurisprudenza e dottrina nel diritto dell'internet*, in *Diritto dell'informazione e dell'informatica*, 2010, fasc. 3, p. 377-389; V. ZENO-ZENCOVICH, *Internet e concorrenza*, in *Diritto dell'informazione e dell'informatica*, 2010, fasc. 4-5, p. 697-705; A. GENTILI, *Internet e antitrust*, in *AIDA*, 1996, p. 45-58; G.M. RICCIO, *Concorrenza sleale e tutela dei consumatori nelle reti telematiche*, in *Diritto dell'informazione e dell'informatica*, fasc. 3, 2006, p. 307-333.

¹⁷⁵ F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit., p. 58 ss.

¹⁷⁶ Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, cit., p. 5.

¹⁷⁷ C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, cit., p. 114 ss.

¹⁷⁸ L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, cit., p. 104.

¹⁷⁹ G. PITRUZZELLA, *Big Data, Competition and Privacy*, cit., p. 25. Cfr. ITMedia Consulting - Università Bocconi, *L'econo-*

riferimento e il servizio specifico, valutando le dinamiche del mercato e tenendo conto non solo della rapida evoluzione della tecnologica ma anche del benessere dei consumatori/utenti/interessati.

Ciononostante non si può non rilevare un elemento di fondo. Ossia l'evidente sforzo e tentativo GDPR di rendere lecito e rispettoso dei diritti delle persone fisiche non solo il trattamento dei dati personali, ma in generale la gestione dei big data effettuata da piattaforme digitali, servizi e moderne tecnologie di profilazione e intelligenza artificiale.

Il GDPR, pur avendo i suoi limiti e problematiche applicative, palesa con principi quali la limitazione della finalità del trattamento, la minimizzazione e la qualità dei dati, nonché istituti come la c.d. *privacy by design* e *by default* e il diritto alla portabilità dei dati, la volontà latente di invertire l'attuale modello di gestione dei dati.

Fino ad oggi le grandi piattaforme digitali hanno basato la loro crescita e consolidamento sulla raccolta quanto più massiccia possibile di dati. Il meccanismo di funzionamento degli algoritmi e le tecnologie di *machine learning* sfruttano proprio l'accumulo incessante e illimitato di quanti più dati possibile per abilitare ulteriori possibilità di sfruttamento dei dati¹⁸⁰. Significativa è, a tal riguardo, la definizione di big data individuata da Bagnoli con riferimento alla finalità del trattamento: « *Big Data is a set of data collected for a determining purpose and reassembled to respond to other needs, providing valuable information, and competitive advantage* »¹⁸¹.

Se questo ha permesso una rapida fioritura di nuovi servizi, sfociando però nel consolidamento delle posizioni di dominanza di pochi soggetti, ci espone oggi ad alcuni rischi¹⁸². Rischi non solo in termini di alterazione della concorrenza o di scorretta gestione dei dati personali, ma anche in termini di risultati non corretti o fuorvianti prodotti dai processi decisionali automatizzati, fino a lesioni dei diritti e dell'incolumità delle persone¹⁸³.

Tale prassi ormai consolidata è proprio ciò che il GDPR mira a cambiare e invertire¹⁸⁴. In questo approccio è inoltre evidente la

nia dei dati. *Tendenze di mercato e prospettive di policy*, cit., p. 196 ss.

¹⁸⁰ Cfr. AGCOM, *Big Data. Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*, 8 giugno 2018, disponibile al link: <https://www.agcom.it/documents/10179/10875949/Studio-Ricerca+08-06-2018/c72b5230-354d-444f-9e3f-5467ca450714?version=1.0>; ITMedia Consulting - Università Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 150 ss.

¹⁸¹ V. BAGNOLI, *The big data relevant market*, cit., p. 84.

¹⁸² FRA - CoE - ECHR - EDPS, *Handbook on European data protection law*, cit., p. 354 ss.

¹⁸³ Si veda EDPS, *Opinion 3/2018 on on line manipulation and personal data*, op. cit.

¹⁸⁴ ITMedia Consulting - Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, cit., p. 98.

diversità normativa tra gli Stati Uniti d'America e l'Unione Europea in materia di privacy. Mentre nel primo la raccolta, il trattamento e lo scambio di dati personali è sostanzialmente permesso, rendendo quindi naturale la raccolta massiva e incontrollata di dati, nel secondo, soprattutto in seguito al GDPR, si cerca di organizzare e rendere più razionale la gestione dei dati per evitare abusi e rischi di diversa natura ¹⁸⁵. Ecco quindi come il GDPR si propone un obiettivo più ambizioso e che trascende il suo ambito di applicazione territoriale. Oltrepassando i confini europei il GDPR mira infatti a instaurare, su scala mondiale, nuove prassi che si basino su una raccolta e trattamento dei dati personali più rispettoso dei diritti fondamentali dell'uomo.

Dunque, principi come quello di limitazione delle finalità più che adottare un'ottica sanzionatoria e riparatoria sembrerebbe mirare a una modifica più profonda delle dinamiche digitali. In un'ottica preventiva e pro-attiva mirano a fare del trattamento per uno o più scopi specifici dei soli dati necessari la regola nella gestione di dati personali.

Ciononostante si potrebbe comunque obiettare che la riduzione della quantità di dati trattabili potrebbe influire negativamente sia sulla possibilità di garantire la sostenibilità di molti dei servizi offerti sia sull'ulteriore sviluppo tecnologico. Questa eventualità è però già considerata dal GDPR che cerca sempre di bilanciare l'esigenza della riservatezza della persona con la libera circolazione dei dati, conferendo flessibilità al sistema di protezione dei dati personali. Il GDPR si pone così nell'ottica di vietare solo quei trattamenti di dati sproporzionati, eccessivi o abnormi, apprestando per tutti gli altri gli strumenti che consentono di bilanciare le esigenze del mercato con i diritti fondamentali.

In conclusione, a prescindere da come il principio di limitazione della finalità vivrà nella "costituzione materiale" ¹⁸⁶ dei rapporti su Internet, si possono considerare in una certa misura apprezzabili le modalità con le quali il GDPR si propone di raggiungere i suoi obiettivi. Tra questi anche una gestione dei big data più sostenibile e rispettosa della dignità della persona ¹⁸⁷. Obiettivo, quest'ultimo, che potrebbe essere meglio raggiunto tramite un'applicazione convergente delle normative coinvolte, a partire da quelle più direttamente interessate quali privacy e competizione, fino a coinvolgere anche altre branche del diritto, come la tutela del consumatore/utente ¹⁸⁸, la normativa in materia di comunicazioni elettroniche o la proprietà intellettuale.

¹⁸⁵ W. KERBER, *Digital markets, data, and privacy: competition law, consumer law and data protection*, cit., p. 14 ss.

¹⁸⁶ C. MORTATI, *La costituzione in senso materiale*, Milano, 1940.

¹⁸⁷ S. RODOTÀ, *La rivoluzione della dignità*, Napoli, 2013 e *Il diritto di avere diritti*, Bari, 2012.

¹⁸⁸ Un ulteriore esempio di convergenza tra la normativa a tutela dei dati

Solo il tempo potrà dirci se tali ambiziosi obiettivi saranno raggiunti.

Abstract

The work exams the principle of purpose limitation regarding to the so called “secondary use of big data”. It aims to identify a remedy to the possibility of an OTT to reusing personal data and, thanks to the accumulation and the mix of other data, offer new services or enter into new market in order to conquer a dominant position exploiting an illicit competitive advantage.

The principle of purpose limitation, pursuant to art. 5 GDPR, is the principle for which personal data must be collected for “specified, explicit and legitimate” purposes (purpose specification) and not be further processed in a way incompatible with those purposes (compatible use).

This and other principles and remedies (such as the data protection by design e by default and the right of data portability) will be examined in a convergent perspective between the data protection and antitrust law. That is in order to demonstrate that, in particular cases, those two disciplines can work together to achieve the same goal of the trust in the digital single market.

personali e quella a tutela dei consumatori è rinvenibile nelle pronunce del Garante per la Protezione dei Dati Personali con riferimento alle clausole abusive. Il Garante ha infatti dichiarato invalide le clausole che richiedono il consenso senza che questo presenti i requisiti minimi previsti dalla normativa *data protection*, ossia senza rispettare le caratteristiche del “consenso informato”. G. RESTA, *Digital platforms and the law*,

cit., p. 245 e ss, che richiama il provvedimento del GPDP 28 maggio 1997 sugli Istituti di credito - Criteri generali in materia di informativa e richiesta del consenso dell'interessato, doc. web n. 40425, commentato da V. ZENO-ZENCOVICH, *Il “consenso informato” e la “autodeterminazione informativa” nella prima decisione del Garante*, in *Corr. Giur.*, 1997, VIII, p. 915-917.