Big data e "tutele convergenti" tra concorrenza, GDPR e Codice del consumo*

Sara Gobbato

Abstract

I big data configurano un asset strategico per le imprese ma il loro trattamento genera al contempo rischi di violazione dei diritti fondamentali degli utenti/consumatori. Interrogandosi su quale sia il livello di tenuta del sistema, l'articolo prende in esame alcuni esempi emblematici del grado di tutela oggi offerto dall'ordinamento giuridico dell'Unione europea e italiano in materia di concorrenza, dati personali e consumatori. Gli esempi mettono in evidenza alcuni limiti degli strumenti di tutela vigenti, i quali non sembrano assicurare in tempi congrui un'adeguata risposta alle istanze del mercato e dei consumatori nei confronti degli operatori di maggiori dimensioni, attivi su scala globale. Al contempo, le prassi decisionali evidenziano il rischio che, in apparente violazione del divieto di *ne bis in idem*, una medesima condotta delle imprese possa essere vagliata da Autorità settoriali diverse, con il conseguente pericolo di vanificare gli investimenti in innovazione generando incertezza ed oneri procedimentali ingiustificati.

Big data are a strategic asset for companies; at the same time, their processing may trigger the violation of the users/consumers' fundamental rights. By questioning the extent of the risks we are currently facing, the article examines some emblematic examples of the degree of protection offered by the EU and Italian legal systems with specific regard to competition, personal data and consumer law. The examples highlight some of the main shortcomings of the applicable legal tools, which do not seem to respond timely to the market and consumers' requests against big players operating worldwide. At the same time, the current legal framework may lead to a situation where different sectoral Authorities decide to open proceedings against the same company in breach of the *ne bis in idem* prohibition. This outcome appears particularly harmful since it could annihilate innovation investments, while generating uncertainty as well as additional unjustified procedural burdens to the detriment of the whole system.

Sommario

* Il presente contributo corrisponde, con alcune integrazioni, al testo dell'intervento svolto in occasione del convegno *JusTech e Industry 4.0, i cambiamenti indotti dalle nuove tecnologie nel diritto delle imprese*, Università degli Studi di Padova, 14 febbraio 2019. Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista.

Keywords

Big data; Concorrenza; GDPR; Consumatori; Codice del consumo

1. Introduzione: la nozione di big data come asset strategico di rilevanza anche costituzionale

Dal 2000 la locuzione "big data" è progressivamente entrata nel linguaggio comune con significati vari e non sempre univoci[1], sino a comparire a pieno titolo tra i neologismi della lingua italiana nel 2012[2].

Secondo chi ha via via puntualizzato i limiti della nozione, «Big Data is the information asset characterized by such a high volume, velocity and variety to require specific technology and analytical methods for its transformation into value»[3]. I big data sono dunque il campo di applicazione dei supercalcolatori e dell'Intelligenza Artificiale, e si differenziano dalla generalità dei dati in virtù di alcune proprietà comuni sintetizzabili in (almeno) quattro V: il Volume dei dati raccolti, la Velocità con i quali sono trattati, la loro Varietà ed infine il Valore economico da essi generato quale causa e conseguenza dell'incremento progressivo delle tre V precedenti.

L'Autorité de la Concurrence in Francia ed il *Bundeskartellamt* in Germania hanno per l'appunto evidenziato congiuntamente come la generazione di valore sia legata allo sviluppo di nuove metodologie che consentono di estrarre «*valuable information from extremely large accumulations of (often unstructured) data*»[4]. In tal senso, i big data sono quindi intrinsecamente legati ai "*big analytics*", ossia alla capacità dei computer di risolvere problemi complessi attraverso l'analisi di grandi moli di informazioni grazie ad algoritmi altrettanto evoluti[5].

[1] Si veda The Economist, *Data, data everywhere, a special report on managing information*, 1 febbraio 2010, ove si legge che «*scientists and computer engineers have coined a new term for the phenomenon: "big data"*».

[2] Si veda la voce "big data" in Vocabolario Treccani.

[3] A. De Mauro, M. Greco, M. Grimaldi, *A Formal Definition of Big Data Based on its Essential Features*, in *Library Review,* 65(3), 2016, 122 ss. Tale definizione è stata ripresa da Organization for Economic Co-operation and Development (OECD), *Big Data: bringing competition policy to the digital era*, DAF/COMP(2016)14, 29-30 novembre 2016, 5.

[4] In tal senso, Autorité de la Concurrence e Bundeskartellamt, *Competition Law and Data*, 10 maggio 2016, 8. Anche in Italia, l'Autorità Garante della Concorrenza e del Mercato, l'Autorità per le Garanzie nelle Comunicazioni ed il Garante per la protezione dei dati personali hanno avviato una indagine congiunta sui big data IC53 con provvedimento n. 26620 del 30 maggio 2018 in Boll. 21/2017, le cui risultanze preliminari sono state pubblicate l'8 giugno 2018, *Indagine conoscitiva sui big data. Analisi della propensione degli utenti online a consentire l'uso dei propri dati a fronte dell'erogazione di servizi. Primi risultati*. Il 10 luglio 2019, le tre Autorità hanno anticipato le *Linee guida e Raccomandazioni di policy sui big data*, in attesa della pubblicazione del report finale.

[5] In tal senso, M.E. Stucke, A.P. Grunes, *Big Data and Competition Policy*, Oxford, 2016, 23.

All'interno dei big data, è possibile individuare il sottoinsieme dei "dati personali" nell'accezione codificata dal Regolamento (UE) 2016/679 (GDPR)[6]. Si tratta di grandi moli di dati riferibili agli individui che, proprio grazie ai *big analytics*, diventano oggetto di analisi volte ad evidenziare bisogni e caratteristiche personali che possono essere addirittura ignoti al singolo interessato[7]. Secondo le indicazioni fornite dall'OECD, nel sottoinsieme dei big data concernenti informazioni di tipo personale rientrano ad esempio i dati anagrafici, gli *user generated contents* (post, commenti, foto ecc.), i dati concernenti le reti di contatti sui social network e quelli relativi alla localizzazione dell'individuo.

Per l'insieme delle caratteristiche proprie, i big data rappresentano dunque un asset strategico di rilevanza non solo economica per le imprese che li detengono, ma anche – ed inestricabilmente – personale per i singoli "interessati", vista l'incidenza potenziale dei *big analytics* sulle libertà individuali di rango costituzionale.

2. Luoghi comuni e timori nel dibattito sui big data

La combinazione di un asset strategico di valore economico crescente con masse di dati personali elaborate dall'Intelligenza Artificiale genera comprensibilmente, nel dibattito corrente, inquietudini sotto più aspetti che vanno dal potere di mercato acquisito dai detentori di big data, sino all'incidenza del fenomeno sulla privacy e sulle libertà degli interessati.

Le preoccupazioni sono in parte rafforzate da alcuni luoghi comuni che, a ben vedere, non corrispondono del tutto alla realtà[8]. Ad esempio, spesso si sente ripetere che i dati siano il nuovo petrolio. In realtà i dati digitali non sono una risorsa scarsa, destinata come il petrolio ad esaurirsi, dovendo essere più correttamente paragonati ad energie rinnovabili, potenzialmente disponibili in grandi quantità e riutilizzabili da più imprese anche simultaneamente in quanto asset non rivale[9]: si pensi, per fare un esempio assai

[6] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE. Come noto, l'art. 4, n. 1 del GDPR definisce il "dato personale" come «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale». Ai sensi dell'art. 9 del GDPR, costituiscono "categorie particolari" di dati personali quei dati «che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

[7] Quanto all'utilizzo dei big data da parte di forze dell'ordine nello svolgimento delle funzioni di protezione della sicurezza pubblica e di prevenzione e repressione del crimine, si veda A. Bonfanti, *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in questa *Rivista*, 3, 2018, 206 ss.

[8] In proposito G. Colangelo, M. Maggiolino, *Big Data as a Misleading Facility*, in *European Competition Journal*, 2017, 13(2), 249 ss.

[9] Sul tema, D.A. Balto, M. *Lane, Monopolizing Water in a Tsunami: Finding Sensible Antitrust Rules for Big Data*, 22 marzo 2016. Si veda anche M. Maggiolino, *I big data e il diritto antitrust*, Milano, 2018, 176, ove l'Autrice

diffuso nella prassi, ai dati relativi alla geolocalizzazione dell'interessato, il quale abbia validamente fornito distinti consensi, in base al GDPR, ad autonome imprese fornitrici delle app presenti sui vari *device* della persona in questione[10].

In secondo luogo, l'accumulazione dei dati, nel rispetto dei diritti ad essi afferenti, non è di per sé una condotta vietata. Anzi, l'accumulazione di big data produce effetti pro-competitivi, stimola la concorrenza tra imprese sulla base del merito e l'innovazione a vantaggio dei consumatori finali: da tale presupposto prendono impulso le politiche pubbliche di valorizzazione delle risorse informative e delle competenze legate ai big data ed ai *big analytics*[11].

In terzo luogo, nonostante l'assonanza, i big data non sono una prerogativa delle Big Tech Firm (i "giganti del Web" quali Google, Facebook, Amazon). I big data sono infatti rinvenibili e possono essere utilizzati con successo nel settore privato, oltre che in quello pubblico[12], nei più diversi comparti economici (dall'energia ai trasporti, dalle banche alle assicurazioni, alla grande distribuzione ecc.).

Se quelli ora citati risultano dei luoghi comuni, è però innegabile che i maggiori operatori dei mercati digitali suscitino particolari timori proprio per la mole di dati a loro disposizione e per l'uso che essi possono fare in particolare dei nostri dati personali.

Tali timori risultano fondati su tre elementi oggettivi. Innanzitutto, le Big Tech sono effettivamente imprese in "posizione dominante" nei mercati rilevanti di riferimento: ad esempio, Google è l'operatore dominante nel mercato dei servizi di ricerca online[13]. La nozione di dominanza implica per l'appunto la capacità, dell'impresa che la acquisisce legittimamente secondo i propri meriti, di godere di un potere di mercato tale da essere in grado di assumere decisioni senza tener conto delle reazioni di concorrenti e consumatori. Da qui la "speciale responsabilità" delle imprese dominanti, alle quali è

evidenza come «gli individui, non essendo vincolati da alcuna esclusiva con le imprese, utilizzano molti siti e strumenti in grado di raccogliere dati, determinando quello che viene di solito denominato come effetto *multi-homing*. Inoltre, questi dati non sono rivali, ossia il fatto che un'impresa li collezioni non impedisce ai suoi rivali di fare altrettanto». In proposito, si veda inoltre V. Zeno-Zencovich, *Do "data markets" exist?*, in *questa Rivista*, 2, 2019, 22 ss.; A. Ottolia, Big data e innovazione computazionale, in *Quaderni di AIDA*, 28, Torino, 2017, 321 ss.; G. Sivinski, A. Okuliar, L. Kjolbye, *Is big data a big deal? A competition law approach*, in *European Competition Law Journal*, 2017, 13, 199 ss., spec. 200.

[10] Esempi invero più complessi di riutilizzabilità dei dati personali attengono alle fattispecie in cui l'interessato abbia fornito il proprio consenso specifico affinché il titolare del trattamento trasferisca i dati ad imprese ad esso legate da vincoli di controllo oppure a soggetti terzi indipendenti. Anche per tali ipotesi, il valido consenso dell'interessato conduce a situazioni in cui più imprese trattano lecitamente i medesimi dati personali, che dunque si confermano come asset per propria natura non necessariamente rivale, vista la "replicabilità" del consenso in favore di soggetti titolari diversi.

[11] Per l'Italia si consideri il Piano nazionale Impresa 4.0 (già Industria 4.0).

[12] La creazione di una piattaforma per la valorizzazione dei dati della PA costituisce uno degli obiettivi perseguiti sin dal *Piano triennale per l'informatica nella PA 2017-2019*, confermato nel successivo Piano 2019-2021 mediante l'implementazione della Piattaforma Digitale Nazionale Dati che mira ad «aprire il mondo della Pubblica Amministrazione ai benefici offerti dalle moderne piattaforme per la gestione e l'analisi dei big data» (in tal senso, AgID, *Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019 – 2021*, 19 marzo 2019, 71).Le azioni intraprese nel contesto italiano si collocano all'interno della strategia di *eGovernment* elaborata a livello di Unione europea nell'ambito della Digital Single Market Strategy (sul tema si veda, per il periodo in corso, la Comunicazione della Commissione europea, *Piano d'azione dell'UE per l'eGovernment 2016-2020. Accelerare la trasformazione digitale della pubblica amministrazione*, COM(2016) 179 final).

[13] In proposito Commissione europea, decisione AT.39740 *Google Search (Shopping)* del 27 giugno 2017.

fatto divieto – come in seguito si vedrà – di abusare del potere che le contraddistingue adottando decisioni non improntate al merito imprenditoriale.
A ciò va aggiunto che le Big Tech hanno fondato il loro successo su modelli di business gratuiti, sul versante dei servizi forniti ai consumatori finali, proprio allo scopo di accumularne i dati: questi ultimi sono il vero asset strategico, sotto il profilo economico, rivenduto lecitamente a prezzi di mercato sul versante degli investitori pubblicitari[14] (per tacer delle altre meno dichiarabili ipotesi di trattamento, che esulano dall'oggetto specifico del presente intervento[15]).
Il quadro si completa considerando la strategia di espansione "*cross-markets*" intrapresa dalle Big Tech al di fuori dei mercati rilevanti sui quali esse sono già dominanti[16]: lo scopo di tale strategia sembrerebbe essere quello di costruire un "ecosistema" in espansione, entro il quale il consumatore può soddisfare i bisogni più diversi senza dover rivolgere altrove la propria domanda[17].
Di fronte al potere di mercato detenuto dalle Big Tech ed all'incidenza espansiva dei loro modelli di business sui dati personali, viene dunque naturale interrogarsi su quale sia il grado di effettività degli strumenti offerti dall'ordinamento giuridico a tutela dell'assetto dei mercati e, quindi, delle libertà degli individui.

3. Facebook/WhatsApp: un caso tre volte emblematico

I modelli di business fondati sullo sfruttamento economico di big data di tipo personale dei consumatori rientrano nel campo di applicazione di vari ambiti normativi: per fermarci all'Unione europea, vengono in rilievo in particolare le disposizioni a tutela dei dati personali (il Regolamento (UE) 2016/679 GDPR e per l'Italia il Codice della Privacy introdotto con il d.lgs. 196/2003), le norme a protezione dei consumatori (il Codice del Consumo adottato con il d.lgs. 206/2005 in attuazione di varie Direttive UE di armonizzazione) e quelle a tutela della concorrenza (in particolare gli artt. 101 e 102 TFUE, il Regolamento 139/2004/CE e, per l'Italia, la legge per la concorrenza e cioè la l. 287/1990)[18].
Soffermandoci sulle disposizioni a tutela della concorrenza, va ricordato che esse, concepite all'epoca dell'analogico, vengono oggi applicate dalle Autorità per la concorrenza (Commissione europea ed Autorità nazionali) nel nuovo contesto digitale secondo

[14] M. Maggiolino, *I big data e il diritto antitrust*, cit., 244-245; M.C. Wasastjerna, *The role of big data and digital privacy in merger review,* in *European Competition Law Journal*, 2018, 14 (2-3), 417 ss., spec. 420.

[15] Il riferimento è, ad esempio, al caso Cambridge Analytica sul quale si vedano D. Susser, B. Roessler, H. Nissenbaum, *Technology, Autonomy, and Manipulation*, in *Internet Policy Review*, 8(2), 2019, 1 ss.; L.J. Trautman, *Governance of the Facebook Privacy Crisis*, 31 marzo 2019, in *SSRN*; A. Pouliou, *Political Profiling: From the US to the EU, Data Protection Regulation from a Transatlantic Perspective*, 3 gennaio 2018, in *SSRN*.

[16] Si pensi ad esempio alla decisione di Amazon, leader nel mercato dei servizi di intermediazione sulle piattaforme e-commerce, di acquisire la catena di negozi di cibi freschi Whole Foods.

[17] M. Maggiolino, *I big data e il diritto antitrust*, cit., 63 e 265.

[18] A ciò vanno aggiunti gli aspetti di tutela del pluralismo informativo, oggetto di regolamentazione da parte dell'AGCOM, che – per necessità di selezione dei temi qui affrontabili – non vengono sviluppati nel presente contributo.

il tradizionale approccio casistico, nei limiti in cui le fattispecie concrete possano essere ricondotte alle nozioni di "intesa", "abuso di posizione dominante" o "concentrazioni tra imprese", di volta in volta rilevanti.

Le regole vigenti in materia di concentrazioni di dimensione europea (Regolamento 139/2004/CE) si sono misurate con i mercati digitali, in particolare, in occasione dell'operazione in esito alla quale Facebook ha acquisito il controllo esclusivo di WhatsApp[19]. Il relativo procedimento di autorizzazione del *merger*, svolto dalla Commissione europea, ha consentito di evidenziare alcuni dei limiti che connotano le disposizioni vigenti. In primo luogo, l'operazione avrebbe potuto non essere notificata alla Commissione europea in quanto l'impresa oggetto di acquisizione non raggiungeva le quote di fatturato richieste per la sussistenza del relativo obbligo ai sensi del Regolamento 139/2004/CE. La concentrazione è stata sottoposta al vaglio della Commissione per effetto del rinvio deciso dalla stessa Facebook al fine di beneficiare dell'*one-stop-shop* a Bruxelles, evitando di dover notificare il *merger* a più Autorità nazionali[20]. L'originaria incompetenza della Commissione è diretta conseguenza del modello di business adottato da WhatsApp, e caratteristico di molte imprese digitali, gratuito per i consumatori e dunque caratterizzato da relativamente bassi livelli di fatturato a fronte dell'ingente mole di dati acquisiti dalla target[21].

Per effetto dell'apparente *gap* nelle competenze della Commissione, ci si è dunque chiesti se occorra riformare il Regolamento 139/2004/CE, al fine di estendere l'obbligo di notifica a quelle operazioni che, pur non raggiungendo i livelli di fatturato ivi stabiliti, presentino un impatto "*cross-border*" in ragione del valore economico del target evidenziato, ad esempio, dal prezzo dell'acquisizione e dal volume dei dati detenuti dall'impresa oggetto della transazione[22].

---

[19] Commissione europea, COMP/M.7217 Facebook/WhatsApp del 3 ottobre 2014. In proposito, si veda E. Ocello, C. Sjödin, A. Subočs, *What's Up with Merger Control in the Digital Sector? Lessons from the Facebook/WhatsApp EU merger case*, in *Competition merger brief*, 2015, 1; G. Pitruzzella, *Big Data and Antitrust Enforcement*, in *Rivista Italiana di Antitrust*, 2017, 1, 77 ss.; M.C. Wasastjerna, *op. cit.*, spec. 427-429; K. Bania, *The role of consumer data in the enforcement of EU competition law*, in *European Competition Journal*, 14(1), 2018, 38 ss.

[20] La concentrazione *Facebook/WhatsApp* è stata autorizzata dalla Commissione europea previa richiesta di Facebook, che si è avvalso della facoltà di rinvio del caso alla Commissione europea quale *best-placed-authority* per l'esame del merger ai sensi dell'art. 4, par. 5, del Regolamento 139/2004/CE.

[21] G. Muscolo, *Big data e Concorrenza. Quale rapporto?*, in V. Falce, G. Ghidini, G. Olivieri (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2018, 173.

[22] In proposito si veda la pubblica consultazione avviata dalla Commissione europea nel 2016, i cui risultati sono pubblicati in *Summary of replies to the Public Consultation on Evaluation of procedural and jurisdictional aspects of EU merger control*, luglio 2017, ove a p. 5 si legge che «*the majority of public and private stakeholders responding to the questionnaire do not perceive any (significant) enforcement gap as regards highly valued acquisitions of target companies that do not generate sufficient turnover to meet the jurisdictional thresholds of Article 1 of the EU Merger Regulation, which would require legislative action. In addition, they consider that the referral mechanism pursuant to Articles 4(5) and 22 of the EU Merger Regulation combined with national merger review systems in the Member States are sufficient to ensure that cases without Union dimension are reviewed either at national or European level. Some respondents note, however, that the extent to which high value/ low turnover transactions could be caught through the referral system depends on the existence of non-turnover-based notification thresholds in at least some Member States*». Si v. altresì il report affidato dalla Commissione europea a J. Crémer, Y. de Montjoye, H. Schweitzer, *Competition policy for the digital era*, Lussemburgo, 2019, 110 ss., ove gli Autori concludono che, al momento, non appare necessario procedere ad un aggiornamento del Regolamento 139/2004/CE; revisioni potrebbero essere adottate in futuro, qualora emergano lacune nel sistema di controllo delle

In secondo luogo, nel caso Facebook/WhatsApp la Commissione europea ha autorizzato il *merger* in "fase 1", ossia senza avviare un'istruttoria approfondita. Le criticità concorrenziali sono state escluse considerando che acquirente e target fossero attive su "mercati rilevanti" diversi (secondo la logica di espansione "*cross-markets*" citata sopra). Secondo la Commissione, inoltre, la concentrazione non avrebbe prodotto, per i concorrenti attuali e potenziali, una minore disponibilità di dati personali, presenti in grandi quantità nel mondo digitale come asset non rivale[23].

Da ultimo quanto agli effetti del *merger* sugli utenti, la Commissione ha espressamente affermato che l'impatto dell'operazione sulla privacy degli individui non rientra nel campo di indagine antitrust, dovendo invece essere valutata in sede di applicazione delle disposizioni sulla protezione dei dati personali[24].

L'istruttoria svolta nel 2014 si è rivelata in seguito non interamente completa: nel 2017, infatti, la Commissione europea ha irrogato una sanzione di 110 milioni di euro a Facebook[25], avendo accertato che quest'ultima aveva omesso informazioni rilevanti in merito alla fattibilità tecnica ed all'intenzione effettiva (poi realizzata nel 2016) di procedere all'abbinamento – tramite *linking/matching* – dei profili WhatsApp e Facebook del medesimo utente[26].

concentrazioni a seguito dell'analisi del meccanismo di rinvio delle operazioni ai sensi del Regolamento 139/2004/CE e delle riforme introdotte in Austria ed in Germania con la previsione di nuovi criteri di notifica basati sul valore della transazione. Sul punto, va evidenziato che nelle già citate *Linee guida e Raccomandazioni di Policy sui big data*, AGCM, AGCOM e il Garante dei dati personali hanno espresso la propria convinzione circa la necessità di rinnovare le regole sul *merger control* tanto a livello nazionale quanto internazionale. Al punto 8 di tali *Linee guida*, le tre Autorità hanno infatti precisato tra l'altro che: «Al fine di aumentare l'efficacia dell'intervento delle autorità di concorrenza rispetto alle operazioni di concentrazione è auspicabile: 1. una riforma a livello nazionale e internazionale che consenta alle autorità di concorrenza di poter valutare pienamente anche quelle operazioni di concentrazione sotto le attuali soglie richieste per la comunicazione preventiva, ma che potrebbero risultare idonee a restringere sin dalla loro nascita importanti forme di concorrenza potenziale (come le acquisizioni da parte dei grandi operatori digitali di start-up particolarmente innovative anche soprannominate "*killing acquisitions*")».

[23] La Commissione ha preso in considerazione il rapporto di *multi-homing* caratterizzante l'utilizzo delle app di *consumer communication* di Facebook e WhatsApp: «*Furthermore, the EEA market for consumer communications apps features a significant degree of "multi-homing", that is, users have installed, and use, on the same handset several consumer communications apps at the same time. In particular, WhatsApp and Facebook Messenger have been reported as being the two main consumer communications apps simultaneously used by the majority of the users in the EEA. This fact suggests that the two consumer communications apps are to some extent complementary, rather than being in direct competition with each other*». In tal senso COMP/M.7217, cit., § 105.

[24] Si veda Commissione europea, COMP/M.7217, cit., § 164: «*For the purposes of this decision, the Commission has analysed potential data concentration only to the extent that it is likely to strengthen Facebook's position in the online advertising market or in any sub-segments thereof. Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules*».

[25] Commissione europea, M.8228 *Facebook/WhatsApp*, 17 maggio 2017.

[26] Quanto alla linea seguita negli USA, in epoca più recente, e precisamente il 6 settembre 2019, l'Attorney General di New York, insieme ad altri otto Stati, ha reso noto di aver avviato un'indagine antitrust congiunta nei confronti di Facebook per abuso di posizione dominante con un impatto sul trattamento dei dati personali e sui diritti dei consumatori. Un'analoga azione è stata avviata nei confronti di Google. In proposito, si vv. i *press release* *AG James Investigating Facebook For Possible Antitrust Violations* del 6 settembre 2019 e *Attorney General James Announces Antitrust Investigation Into Google* del 9 settembre 2019.

4. L'approccio seguito dal *Bundeskartellamt* ai sensi della GWB

L'integrazione di Facebook/WhatsApp diventa sempre più paradigmatica anche considerando i diversi approcci ad essa via via applicati dalle Autorità nazionali.
A conclusione di un procedimento iniziato nel 2016, il 6 febbraio 2019 l'Autorità per la concorrenza tedesca ha emesso una decisione nei confronti di Facebook[27] per abuso della posizione dominante ai sensi dell'art. 19 della legge nazionale a tutela della concorrenza (GWB)[28]. L'abuso è stato accertato con riferimento al mercato tedesco dei servizi di social network destinati agli utenti privati, sul quale Facebook detiene una quota superiore al 95% degli utenti attivi giornalmente in Germania[29].
Nell'individuare il mercato rilevante, il *Bundeskartellamt* ha fatto applicazione di alcune novità introdotte nella legge tedesca proprio per tener conto delle peculiarità delle piattaforme online. Si tratta in particolare degli art. 18(2a) e (3a) GWB, i quali consentono all'Autorità di individuare un "mercato rilevante" anche in relazione a servizi forniti gratuitamente ai consumatori finali in assenza di un "prezzo". Le novità introdotte consentono inoltre di esaminare la posizione detenuta dalle imprese attive su "mercati a più versanti" (come sono le piattaforme di social network tramite le quali interagiscono, dai rispettivi "versanti", gli utenti finali, gli sviluppatori di app e di servizi, gli inserzionisti pubblicitari e gli editori di contenuti) considerando vari aspetti: gli effetti di rete diretti ed indiretti; l'utilizzo parallelo, da parte del medesimo consumatore, di servizi offerti da diversi *provider*; gli eventuali *switching cost* per il passaggio ad un nuovo operatore; le economie di scala godute dal *provider* in relazione agli effetti di rete; la pressione concorrenziale *innovation-driven*; la disponibilità di dati idonei ad assicurare un vantaggio competitivo.
In applicazione della GWB così aggiornata, il *Bundeskartellamt* ha accertato che Facebook avrebbe abusato della propria posizione dominante nel mercato tedesco dei social network proprio per le modalità di trattamento dei dati personali acquisiti tramite WhatsApp, Instagram, Oculus, Masquerade e siti web di terzi collegati tramite *plug in* (la funzione "*like*" di Facebook). In applicazione della propria *data policy*, Facebook avrebbe imposto agli utenti (senza che questi abbiano fornito un libero consenso al riguardo ai sensi dell'art. 6 GDPR) di fondere nel profilo *Facebook.com* tutti i dati personali provenienti dalle varie fonti, al fine di sfruttarli per scopi commerciali. Secondo le pronunce del *Bundesgerichtshof* nei casi *VLB-Gegenwert* e *Pechstein* citati dal *Bundeskartellamt*, l'imposizione di clausole contrattuali sbilanciate in favore del "contraente forte", e nella fattispecie di una *data policy* contraria all'art. 6 GDPR in danno degli utenti,

[27] Si veda Bundeskartellamt, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*, 15 February 2019.

[28] *Gesetz gegen Wettbewerbsbeschränkungen* (GWB).

[29] Secondo quanto notato dal *Bundeskartellamt*, tale quota di mercato connota una stabile posizione dominante in ragione dei forti effetti di rete di tipo diretto, che rendono assai difficile per l'utente attivo su Facebook passare ad un'altra piattaforma trasferendo su di essa tutti i propri contatti social. A ciò si aggiunge il fatto che Facebook per definizione, in quanto piattaforma social, dispone di dati personali altamente rilevanti in termini competitivi, in quanto asset indispensabile per la commercializzazione di servizi pubblicitari personalizzati.

configura di per sé una violazione non solo del GDPR ma anche del divieto di abuso di posizione dominante ai sensi dell'art. 19(1) GWB. Su tali basi, il *Bundeskartellamt* ha quindi ordinato a Facebook di modificare i termini d'uso del proprio servizio ponendo fine alla condotta entro dodici mesi.
In un primo comunicato a caldo sulla decisione, Facebook ha contestato le conclusioni raggiunte dall'Autorità ed in particolare la sussistenza della competenza del *Bundeskartellamt* in tema di applicazione del GDPR, rilevando che, nella fattispecie, essa spetterebbe semmai all'*Irish Data Protection Commission* (in ragione dello Stato dell'Unione ove ha sede la controllata Facebook Ireland Ltd.)[30].

5. L'approccio dell'AGCM in base al Codice del consumo

La modifica delle condizioni d'uso di WhatsApp a seguito dell'acquisizione del controllo da parte di Facebook è stata oggetto d'attenzione da parte anche dell'Autorità Garante della Concorrenza e del Mercato (AGCM), che nell'ordinamento italiano tutela sia la concorrenza sia i consumatori in applicazione del Codice del consumo.
Con un primo provvedimento, nel maggio 2017[31] l'AGCM ha irrogato a WhatsApp una sanzione di 3 milioni di euro per una pratica commerciale scorretta di tipo aggressivo ai sensi degli artt. 20, 24 e 25 del Codice del consumo, concernente la modifica delle condizioni generali di contratto. Secondo gli accertamenti dell'Autorità, nell'agosto 2016 WhatsApp avrebbe indotto i propri utenti ad accettare integralmente le modifiche apportate ai termini di utilizzo dell'applicazione WhatsApp Messenger, pre-impostando l'opzione che consente la condivisione con Facebook di alcuni dati personali a fini di profilazione commerciale e pubblicitari. In caso di mancata accettazione sarebbe stata prospettata l'interruzione del servizio[32].
L'AGCM ha respinto le difese di WhatsApp, che nel corso dell'istruttoria aveva sostenuto tra l'altro che l'Autorità dovesse sospendere il procedimento sin tanto che il Garante della Privacy non si fosse pronunciato sulla fattispecie in merito alla liceità del trasferimento dei dati. A tale riguardo, l'AGCM ha affermato che «[i]n linea di principio, la circostanza che alla condotta della Parte sia applicabile il Codice della privacy, non la esonera dal rispettare le norme in materia di pratiche commerciali scorrette, che rimangono applicabili con riferimento alle specifiche condotte poste in essere dal Professionista, finalizzate all'acquisizione del consenso alla condivisione dei dati personali».

[30] Y. Cunnane, N. Shanbhag, *Why We Disagree With the Bundeskartellamt*, 7 febbraio 2019.

[31] AGCM, provv. n. 26597, PS10601 – *WhatsApp-Trasferimento dati a Facebook*, 11 maggio 2017, in Boll. 18/2017.

[32] Con un secondo provvedimento sempre relativo a WhatsApp Messenger, l'AGCM ha accertato il carattere vessatorio e, dunque, la nullità ai sensi degli artt. 33 e 35 del Codice del consumo di alcune clausole del modello contrattuale sottoposto agli utenti, che assicuravano a WhatsApp, tra l'altro, esclusioni e limitazioni di responsabilità ampie e generiche, la possibilità di interrompere unilateralmente il servizio o di variare le condizioni d'uso senza motivo e senza preavviso, l'applicazione della legge della California e l'individuazione dei Tribunali dello stesso Stato quali unici fori competenti per la risoluzione delle controversie. Si veda AGCM, provv. n. 26596, CV154 – *WhatsApp – Clausole Vessatorie*, 11 maggio 2017, in Boll. 18/2017.

Con un ulteriore provvedimento del 2018[33], l'AGCM ha sanzionato Facebook per complessivi 10 milioni di euro per due pratiche commerciali scorrette, poste in essere nei confronti degli utenti italiani in violazione del Codice del consumo.

In primo luogo, secondo l'AGCM, Facebook avrebbe posto in essere una pratica ingannevole, vietata dagli artt. 21 e 22 del Codice del consumo, adottando una carente informativa nella fase di prima registrazione dell'utente nella piattaforma (sito web e app). Facendo leva sul *claim* «Iscriviti, è gratis e lo sarà per sempre», Facebook avrebbe informato gli utenti esclusivamente della gratuità del servizio, senza evidenziare le finalità commerciali di utilizzo dei dati raccolti.

Nel corso del procedimento, Facebook ha sostenuto che la fornitura di servizi "gratuiti" (quali sono i servizi del Social Network per gli utenti) non darebbe luogo ad un'attività economica rilevante ai sensi del Codice del consumo. Nel rigettare tale tesi, l'AGCM ha confermato che l'uso dei dati degli utenti per finalità di marketing configura un «rapporto di consumo tra il Professionista e l'utente che utilizza i servizi di [Facebook] (tramite sito e app), anche in assenza di corrispettivo monetario», risultando dunque confermato che i dati degli utenti sono a tutti gli effetti una «controprestazione non pecuniaria»[34]. Nella fattispecie, secondo l'AGCM, l'ingannevolezza sarebbe risultata inoltre aggravata dalla circostanza che «nell'uso di [Facebook], le finalità commerciali si prestano ad essere confuse con le finalità sociali e culturali, tipiche di un social network»[35].

Quanto alla seconda condotta accertata, l'AGCM ha rilevato che Facebook avrebbe posto in essere una pratica aggressiva, vietata dagli artt. 24 e 25 del Codice del consumo, nei confronti degli utenti registrati, i cui dati sarebbero stati trasmessi dalla piattaforma social ai siti web/app di terzi e viceversa senza preventivo consenso espresso dell'interessato, per finalità di profilazione e commerciali. L'AGCM ha accertato che tale trasmissione inconsapevole sarebbe stata resa possibile poiché Facebook preimposta il consenso dell'utente a tale condivisione, preselezionando la funzione di "attivazione della Piattaforma". A fronte della preimpostazione automatica della funzione, l'utente avrebbe una mera facoltà di *opt-out*, che viene disincentivata prospettando conseguenze penalizzanti sia nella fruizione di Facebook, sia nell'accessibilità ed utilizzo di siti web e app di terzi.

Nel corso del procedimento, Facebook ha eccepito l'incompetenza dell'AGCM, rilevando che l'Autorità agirebbe «al di là delle proprie competenze nella misura in cui utilizza le norme a tutela del consumatore per analizzare condotte che dovrebbero essere valutate sulla base della normativa sulla privacy e sul trattamento dei dati personali»[36]. Analogamente a quanto sostenuto dinanzi al *Budneskartellamt*, anche dinanzi all'Autorità italiana Facebook ha rilevato quindi che la competenza ad accertare i fatti contestati spetterebbe *all'Irish Data Protection Commission* e non all'AGCM.

Nel respingere l'eccezione, l'AGCM ha confermato la propria competenza ribadendo

[33] AGCM, provv. n. 27432, PS11112 – *Facebook-Condivisione dati con terzi*, 29 novembre 2018 in Boll. 46/2018.

[34] *Ivi*, § 54.

[35] *Ivi*, § 55.

[36] *Ivi*, § 34.

che «la circostanza che alle condotte della società [Facebook] sia applicabile la normativa sulla privacy, non la esonera dal rispettare le norme in materia di pratiche commerciali scorrette». Mentre la disciplina della privacy, affidata al Garante, tutela i dati personali, «il Codice del Consumo, in materia di pratiche commerciali scorrette, ha l'obiettivo di tutelare il consumatore da scelte economiche indotte da pratiche ingannevoli e aggressive che non trovano regolazione in specifiche discipline». Secondo l'AGCM, dunque, «le due discipline hanno un campo di applicazione materiale differente e perseguono interessi distinti. Di conseguenza non sussiste un conflitto tra le due discipline, integrandosi, piuttosto, le stesse in maniera complementare»[37].
Quanto al rilievo nella fattispecie dei big data detenuti da Facebook, va ricordato che – ai fini dell'accertamento delle pratiche scorrette – è sufficiente che la condotta sia idonea a falsare in misura apprezzabile il comportamento economico del consumatore medio; l'entità dei consumatori interessati (nella fattispecie, i 31 milioni di utenti italiani di Facebook) e, quindi indirettamente, il volume dei dati personali interessati, assumono rilievo ai fini della determinazione della gravità della violazione accertata e del calcolo della relativa sanzione, per legge contenuta entro il tetto massimo di 5 milioni di euro per ciascuna pratica accertata[38].

6. Criticità in tema di effettività e *ne bis in idem*

Gli esempi forniti sembrano indicare un fatto: i diversi strumenti di tutela a disposizioni delle Autorità (GDPR, norme a tutela della concorrenza e dei consumatori) tendono a convergere ed a sovrapporsi sulle medesime condotte delle imprese.
L'applicazione convergente, per quanto sin qui riportato, non sembrerebbe tuttavia tradursi in procedimenti e provvedimenti finali pienamente efficaci a tutela del mercato e dei consumatori. Il caso Facebook rende evidenti alcuni dei limiti al riguardo riscontrabili: il numero delle diverse Autorità procedenti in diversi Paesi su analoga fattispecie; la durata delle istruttorie; gli importi relativamente limitati (considerate le dimensioni economiche dell'impresa interessata) delle sanzioni cumulate nei vari pro-

[37] *Ivi*, § 46.

[38] Avendo accertato due condotte distinte «dotate di autonomia strutturale e funzionale» (cfr. il già citato provv. n. 26597, § 74), l'AGCM ha applicato due sanzioni (secondo il c.d. "cumulo materiale"), nella misura edittale massima di 5 milioni di euro per la prima pratica ingannevole e di ulteriori 5 milioni di euro per la seconda pratica aggressiva. La quantificazione della sanzione è avvenuta considerate la particolare gravità delle pratiche accertate, la loro estensione (riguardante come detto tutti i 31 milioni di utenti italiani del Social Network) e la relativa durata (ancora in corso dal 2008 alla data del provvedimento). Alla data di redazione della presente nota, è in corso il giudizio proposto dinanzi al Tar Lazio da Facebook per l'annullamento del provvedimento dell'AGCM. Il Tar ha in particolare accolto l'istanza di sospensione del provvedimento limitatamente alla parte in cui questo poneva a carico di Facebook l'obbligo di pubblicare una dichiarazione rettificativa riguardo l'utilizzo dei dati personali degli utenti, «in considerazione delle difficoltà tecniche prospettate, anche in ordine ai tempi necessari per la completa ottemperanza». Si veda Tar Lazio, sez. I, ordd. 16 gennaio 2019, nn. 335 e 336. Con successiva ord. 2 maggio 2019, n. 5527, il Tar ha rinviato la causa all'udienza del 18 dicembre 2019, ordinando a Facebook di fornire chiarimenti in merito agli impegni assunti dinanzi alla Commissione europea quanto alla modifica dei termini d'uso del servizio, a seguito dell'azione congiunta avviata dal *Consumer Protection Cooperation Network* (al quale si accennerà al par. 7 della presente nota), e che dovrebbero trovare attuazione nel mese di giugno dello stesso anno.

cedimenti; la marginale o carente valutazione della mole di dati oggetto delle condotte controverse.

Alla limitata efficacia del sistema per gli operatori dotati di maggiori risorse per fronteggiare procedimenti ed eventuali sanzioni, si accompagna d'altro canto un rischio per la generalità delle imprese che decidano di investire nei big data, legato alla possibile violazione del principio del *ne bis in idem* riconosciuto dall'art. 4 del Protocollo n. 7 della Convenzione europea per i diritti dell'uomo e dall'art. 50 della Carta dei diritti fondamentali dell'Unione europea[39]: l'applicazione convergente genera infatti il rischio che, per la medesima condotta, una stessa impresa possa essere chiamata a rispondere da più Autorità anche all'interno della medesima giurisdizione nazionale, così aumentando il grado complessivo di incertezza ed i costi di *compliance* addossati agli operatori economici.

Va ricordato che il principio del *ne bis in idem* (che vieta specificamente, in ambito penale, la «ripetizione di un procedimento conclusosi con una decisione definitiva riguardante il medesimo elemento materiale»[40]) trova applicazione in considerazione del carattere punitivo delle sanzioni irrogabili dalle Autorità amministrative indipendenti[41]. Sotto il profilo formale, non presentano carattere penale gli illeciti sanzionati da norme che, come ad esempio la l. 287/1990 o il Codice del consumo, perseguono la tutela di interessi diversi, quali appunto la tutela della concorrenza e dei consumatori, non riconducibili alla sfera penale. Nondimeno, le ammende irrogate dall'AGCM possiedono sostanzialmente carattere penale, secondo quanto chiarito dalla Corte europea dei diritti dell'uomo, in quanto perseguano il duplice obiettivo di prevenire e di reprimere le condotte illecite realizzate dalle imprese, mediante l'irrogazione di sanzioni di carattere punitivo[42].

---

[39] L'art. 50 della Carta dei diritti fondamentali dell'Unione europea sancisce che «[n]essuno può essere perseguito o condannato per un reato per il quale è già stato assolto o condannato nell'Unione a seguito di una sentenza penale definitiva conformemente alla legge».

[40] CGUE, C- 617/17, *Powszechny Zakład Ubezpieczeń na Życie S.A.* (2019), § 32.

[41] In proposito, B. Nascimbene, *Ne bis in idem, diritto internazionale e diritto europeo*, in *Diritto penale contemporaneo*, 2 maggio 2018; R. D'Ambrosio, *Commento all'art. 50 Carta dei diritti fondamentali dell'Unione europea*, in R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, 1015 ss.; A. Longo, F.M. Distefano, *La storia infinita del ne bis in idem e del doppio binario sanzionatorio*, in *Federalismi.it*, 28 giugno 2017; B. Lavarini *Il fatto ai fini del ne bis in idem tra legge italiana e CEDU: la Corte Costituzionale alla ricerca di un difficile equilibrio*, in *Processo penale e giustizia*, 1, 2017, 60 ss.; E. Pezzi, *I due volti del ne bis in idem alla luce delle influenze europee*, in *Archivio penale*, 2018, 9; F. Viganò, *La Grande Camera della Corte di Strasburgo su ne bis in idem e doppio binario sanzionatorio*, in *Diritto penale contemporaneo*, 18 novembre 2016. Sul tema, si veda ad es. Cons. Stato, sez. VI, 20 settembre 2018, n. 6795: «il principio del *ne bis in idem*, [ai sensi del]l'art. 4 del protocollo n. 7 della CEDU implica soltanto la tendenziale messa al bando del c.d. "doppio binario" sanzionatorio, vale a dire della previsione, per il medesimo fatto, di sanzioni di natura distinta (sul piano della qualificazione interna) applicabili alla stessa persona tramite procedimenti di diverso tipo, essendo la violazione della norma convenzionale innescata non dalla mera pendenza contemporanea di due procedimenti, ma dal fatto che uno di essi venga instaurato o prosegua dopo che l'altro si sia chiuso con una decisione definitiva, non importa se di assoluzione o di condanna».

[42] CEDU, *A. Menarini Diagnostics Srl c. Italia*, ric. 43509/08 (2011). Secondo la Corte europea dei diritti dell'uomo, «al fine di stabilire la sussistenza di una "accusa in materia penale", occorre tener presente tre criteri: la qualificazione giuridica della misura in causa nel diritto nazionale, la natura stessa di quest'ultima, e la natura e il grado di severità della 'sanzione'». In tal senso, CEDU, *Grande Stevens e altri c. Italia*, ricc. 18640/10, 18647/10, 18663/10, 18668/10 e 18698/10 (2014), § 94. Su tale pronuncia,

Ciò posto, va peraltro aggiunto che il *ne bis in idem* non osta a che l'ordinamento giuridico nazionale preveda risposte repressive complementari in relazione ad un medesimo fatto lesivo di beni giuridici distinti, attribuendo le rispettive competenze ad Autorità fra loro autonome[43].

Anzi, come chiarito dalla stessa Corte europea dei diritti dell'uomo, l'imposizione, da parte di Autorità differenti, di distinte sanzioni sulla medesima condotta, è compatibile con il suddetto principio in presenza di determinati presupposti: occorre verificare, in particolare, che i "procedimenti convergenti" perseguano obiettivi complementari non solo in senso astratto, ma anche in concreto, avuto cioè riguardo ai distinti aspetti oggetto di autonomo accertamento in merito alla condotta illecita in rilievo[44].

Per evitare che la plurioffensività di una condotta si traduca in automatismi basati su asserzioni meramente formali, in conformità al *ne bis in idem* ciascuna Autorità è dunque tenuta ad accertare i «profili autonomi di iniquità»[45] nell'esercizio delle specifiche competenze ad essa attribuite.

Per raggiungere tale esito assicurando il sostanziale rispetto dei diritti fondamentali dei soggetti sottoposti al procedimento, oltre a verificare la portata astrattamente complementare delle disposizioni in rilievo circa una medesima condotta, occorre quindi che l'Autorità accerti e fornisca adeguata motivazione in ordine all'elemento oggettivo distintivo a base della rispettiva competenza.

L'effettiva applicazione degli strumenti di tutela in tema di big data di natura anche personale non può prescindere, infatti, dalla preliminare applicazione del divieto di *bis*

M. Allena, *Il caso grande Stevens contro Italia: le sanzioni CONSOB alla prova dei principi CEDU*, in *Giornale di Diritto Amministrativo,* 11, 2014, 1053 ss.; G. De Amicis, *Ne bis in idem e doppio binario sanzionatorio: prime riflessioni sugli effetti della sentenza Grande Stevens nell'ordinamento italiano*, in *Diritto penale contemporaneo. Rivista trimestrale*, 3-4, 2014, 201 ss.; G. Guizzi, *La sentenza CEDU del 4 marzo 2014 ed il sistema delle potestà sanzionatorie delle autorità amministrative indipendenti: sensazioni di un civilista*, in *Il Corriere Giuridico,* 11, 2014, 1321 ss.; B. Lavarini, *Corte europea dei diritti dell'uomo e ne bis in idem: la crisi del doppio binario sanzionatorio*, in *Diritto penale e processo*, 12, 2014, 82 ss.; F. Viganò, *Doppio binario sanzionatorio e ne bis in idem: verso una diretta applicazione dell'art. 50 della Carta? (a margine della sentenza Grande Stevens della Corte EDU)*, in *Diritto penale contemporaneo*, 30 giugno 2014.

[43] CEDU, *A e B c. Norvegia*, ricc. 24130/11 e 29758/11 (2016), spec. § 121: «*In the view of the Court, States should be able legitimately to choose complementary legal responses to socially offensive conduct (such as non-compliance with road-traffic regulations or non-payment/evasion of taxes) through different procedures forming a coherent whole so as to address different aspects of the social problem involved, provided that the accumulated legal responses do not represent an excessive burden for the individual concerned*».

[44] CEDU, *A e B c. Norvegia*, cit., §§ 131-132: «*As regards the conditions to be satisfied in order for dual criminal and administrative proceedings to be regarded as sufficiently connected in substance and in time and thus compatible with the bis criterion in Article 4 of Protocol No. 7, the relevant considerations deriving from the Court's case-law, as discussed above, may be summarised as follows. Material factors for determining whether there is a sufficiently close connection in substance include: (i) whether the different proceedings pursue complementary purposes and thus address, not only in abstracto but also in concreto, different aspects of the social misconduct involved; (ii) whether the duality of proceedings concerned is a foreseeable consequence, both in law and in practice, of the same impugned conduct (idem); (iii) whether the relevant sets of proceedings are conducted in such a manner as to avoid as far as possible any duplication in the collection as well as the assessment of the evidence, notably through adequate interaction between the various competent authorities to bring about that the establishment of facts in one set is also used in the other set; (iv) and, above all, whether the sanction imposed in the proceedings which become final first is taken into account in those which become final last, so as to prevent that the individual concerned is in the end made to bear an excessive burden, this latter risk being least likely to be present where there is in place an offsetting mechanism designed to ensure that the overall amount of any penalties imposed is proportionate*».

[45] M. Maggiolino, *I big data e il diritto antitrust*, cit., 150-151 e 157-159.

in idem, onde evitare che l'incertezza ed i conseguenti oneri per le imprese vanifichino ogni incentivo alla concorrenza ed all'innovazione.

7. Possibili soluzioni

Possibili soluzioni per le criticità riscontrate sembrano emergere proprio dagli sviluppi che hanno interessato il caso Facebook negli ultimi mesi. Le autorità nazionali a tutela dei consumatori, riunite nel *Consumer Protection Cooperation Network* (CPC), hanno infatti avviato, ai sensi del Regolamento (CE) 2006/2004[46], un'azione coordinata che, ad aprile 2019, ha condotto Facebook ad impegnarsi formalmente dinanzi alla Commissione europea a modificare i termini d'uso del proprio servizio, per superare entro il mese di giugno 2019 le problematiche rilevate[47]. L'azione congiunta delle autorità nazionali sotto il coordinamento della Commissione nell'ambito del CPC può essere replicata in materia antitrust dallo *European Competition Network*, ed in materia di protezione dei dati personali dallo *European Data Protection Board*.

L'instaurazione di meccanismi stabili di coordinamento a livello di Unione europea sembra, dunque, la chiave per assicurare l'intervento efficace degli Stati membri di fronte ad operatori attivi su scala sovranazionale.

Nello stesso senso, quanto alla necessità del miglior coordinamento in sede non solo di *public enforcement* ma anche di *advocacy*, depongono a livello nazionale le *Linee Guida e Raccomandazioni di Policy sui big data* anticipate da AGCM, AGCOM e Garante per la protezione dei dati personali, che intendono istituire una cooperazione tra loro permanente a partire dalla sottoscrizione di uno specifico *memorandum of understanding*[48].

Oltre che attraverso l'effettiva implementazione di procedure di coordinamento tra le diverse autorità settoriali, i rischi di violazione del principio del *ne bis in idem* potranno essere ridotti qualora sul punto sia applicato un più intenso standard di motivazione dei provvedimenti adottati, circa i requisiti oggettivi distintivi posti a fondamento della rispettiva competenza. A tal riguardo, rimane poi compito delle Corti, a conclusiva garanzia del sistema in sede di sindacato giurisdizionale dei provvedimenti assunti, vigilare sui limiti delle rispettive aree di intervento nell'interpretazione della legge, alla ricerca del miglior bilanciamento tra i diritti fondamentali di consumatori ed imprese.

[46] Regolamento (CE) n. 2006/2004 del parlamento Europeo e del Consiglio, del 27 ottobre 2004, sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa che tutela i consumatori («Regolamento sulla cooperazione per la tutela dei consumatori»), in GUUE L 364 del 9 dicembre 2004, 1–11.

[47] In proposito, si veda il seguente comunicato stampa della Commissione europea: *Su richiesta della Commissione europea e delle autorità di tutela dei consumatori, Facebook modifica le proprie condizioni d'uso e chiarisce come vengono utilizzati i dati dei consumatori*, IP/19/2048 del 9 aprile 2019.

[48] Si vedano le già citate *Linee guida e Raccomandazioni di Policy sui big data*, ove al punto 11 si legge tra l'altro che «le tre Autorità, nell'esercizio delle competenze complementari ad esse assegnate e che contribuiscono a fronteggiare le criticità dell'economia digitale, si impegnano a strette forme di collaborazione negli interventi che interessano i mercati digitali, anche attraverso la sottoscrizione di un *memorandum of understanding*».