JUS CIVILE

TIZIANA RUMI

Professoressa aggregata di Diritto privato – Università degli Studi Mediterranea di Reggio Calabria

PRATICHE COMMERCIALI SCORRETTE PER ILLECITO TRATTAMENTO DEI DATI PERSONALI

SOMMARIO: *1. Introduzione. – 2. Il* business model *dei social network: lo scambio dei servizi contro dati. – 3. L'utilizzo dei dati senza il consenso dell'interessato per fini commerciali quale possibile pratica commerciale scorretta nei provvedimenti dell'AGCM Facebook (2018) e Meta Platforms Ireland Ltd (2024). – 4. ... e quale ipotesi di violazione della concorrenza tra imprese nelle pronunce della Corte di giustizia UE. – 5. Considerazioni conclusive.*

1. – Una specola da cui indagare le problematiche concernenti le pratiche commerciali scorrette è rappresentata dai modelli negoziali cc.dd. «servizi contro dati», sempre più favoriti dal crescente sviluppo dell'economia digitale [1]. La protezione dei dati personali infatti, per un verso, rientra tra i diritti fondamentali garantiti alla persona e, per altro verso, viene sempre più in gioco per il valore economico che il dato personale incorpora [2]. Il processo di digitalizzazione è presente in tutte le attività umane

[1] Secondo un'immagine diffusa i dati sono considerati come il carburante (*new oil*) della nuova economia digitale, sebbene parte della dottrina (A.M. PINELLI, *La circolazione dei dati personali tra tutela della persona, contratto e mercato*, in *Nuova giur. civ. comm*., 6/2022, 1322) consideri l'analogia con il petrolio fuorviante in quanto i dati costituiscono un bene diverso da tutti gli altri vuoi per la loro idoneità ad essere utilizzati e sfruttati contemporaneamente e in luoghi diversi, vuoi per la circostanza che i dati sono inesauribili e vengono generati a ritmi esponenziali.

[2] Dalla prima direttiva sulla protezione dei dati personali contenute in banche dati (del 1995) al Regolamento europeo sulla protezione dei dati personali (del 2016) si è assistito al passaggio dall'idea dei dati personali in termini di diritti soggettivi assoluti, meritevoli di una tutela risarcitoria extracontrattuale in caso di lesione al pari degli attributi della persona, all'idea che i dati personali, costituiscano anche una risorsa economica e che possano essere ceduti come merce di scambio e che i limiti posti al loro trattamento servano a regolamentare una nuova merce in una società centrata sulle "informazioni", dove si passa "dalla protezione di un'integrità non in vendita alla disciplina di una proprietà suscettibile di essere ceduta" (cfr. S. SIMITIS, *Il contesto giuridico e politico della tutela della* privacy, in *Riv. crit. dir. priv*., 4/1997, 575). Il legislatore italiano, tuttavia, ha stentato ad ammettere la libera circolazione dei dati personali tanto che, nonostante la direttiva del 1995 ritenesse funzionale al perseguimento dei propri fini assicurare contemporaneamente la libera circolazione dei dati personali e la salvaguardia dei diritti fondamentali della persona, la legge italiana n. 675 del 1996 era riluttante ad ammettere «che sull'attività contrattuale svolta nel fenomeno dei dati personali insistessero, per la natura così speciale del bene, due discipline, in ragione della coesistenza in quella vicenda negoziale, di situazioni soggettive relative ed assolute, un diritto delle obbligazioni ed un diritto assoluto della personalità» (così V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inf*., 4-5/2018, 695). Questa tendenza trovava conferma, peraltro, anche nella dottrina dell'epoca, poco propensa ad indagare il fenomeno del trattamento dei dati personali anche in chiave economica e di mercato (vedi le considerazioni di S. RODOTÀ, *Conclusioni*, nel volume di V. CUFFARO-V. RICCIUTO-V. ZENO-ZENCOVICH, *Trattamento dei dati e tutela della persona*, Milano, 1998, 308). Con il *General Data Protection Regulation* (GDPR) prima, e con la direttiva 770/2019/UE, poi, la questione relativa alla commercializzazione dei dati personali sembra, tuttavia, ritenersi supe-

ISSN 2281-3918/2421-2563

ed «il contratto diviene strumento di fruizione sia di contenuti, correlati all'utilizzo di strumenti sempre più *smart*, sia di servizi che, lungi dall'essere di utilizzo sporadico, scandiscono le abitudini delle persone e spesso ne condizionano l'esistenza (si pensi all'uso massivo dei *social networks*)» [3].

In questo quadro, la tutela viene affidata sia ai principi ed alle regole che governano il trattamento dei dati (come il principio di lealtà, ma anche quello di proporzionalità, tenuto conto del fatto che è necessario contemperare il diritto alla protezione dei dati con altre libertà costituzionali come la libertà di espressione o di impresa), sia ad altre regole a protezione del consumatore che mirano alla correttezza della pubblicità e delle transazioni commerciali non solo nel suo interesse ma anche nell'interesse del mercato [4]. La sintesi tra queste discipline rappresenta il superamento dell'antico dualismo tra "concezione morale" dei dati personali (che ne esalta la correlazione con l'identità della persona e la sua dignità e libertà) e la concezione patrimoniale dei medesimi (alla stregua della quale i dati possono essere considerati come dei beni e circolare liberamente nel mercato) [5].

La prospettiva attuale, infatti, riconosce l'appartenenza della protezione dei dati personali anche all'ambito negoziale, oltre che a quello dei diritti della personalità, e, a determinate condizioni, ne ammette la circolazione [6]. Ciò presuppone, ovviamente, la qualificazione dei dati personali come beni

---

rata. Lo scambio economico così realizzato corrisponde ad una struttura giuridica di tipo contrattuale, sebbene non si faccia riferimento ad uno specifico contratto (vedi art. 3, par. 2, Direttiva 770/2019/UE). Ciò è messo bene in luce dalla dottrina che individua nel Regolamento una certa «enfasi sul momento circolatorio dei dati personali, rispetto alla sottolineatura delle implicazioni personalistiche del dato personale» (F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm*., 2/2017, 375) e «un diverso bilanciamento degli interessi, che opera in favore della circolazione e con una retrocessione della tutela personalistica» (A. IULIANI, *Note minime in tema di trattamento dei dati personali*, in *Eur. dir. priv*., 1/2018, 302). Nell'ottica della qualificazione del GDPR come disciplina del mercato dei dati personali cfr., anche, N. ZORZI GALGANO, *Le due anime del GDPR e la tutela del diritto alla privacy*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di Zorzi Galgano, Padova, 2019, 35 ss.

[3] Cfr. A. ADDANTE, *La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali*, in *Giust. civ*., 4/2020, 892.

[4] Ciò a conferma del fatto che il dato personale ha anche una dimensione contrattuale e diviene parte della promessa obbligatoria. Peraltro il rilievo economico dei dati personali aumenta il ventaglio di tutele dei singoli consumatori e delle imprese concorrenti, rispetto alla protezione ricavabile dal GDPR, perché garantisce «in astratto di intervenire sulle attività di raccolta, accumulo e trattamento multiplo idonee a consolidare posizioni dominanti e precludere lo sviluppo e l'accesso a servizi maggiormente sensibili ai profili della privacy digitale, anche nelle ipotesi in cui il trattamento sia lecito, ad esempio poiché i dati sono stati sottoposti in via preventiva a procedure di pseudonimizzazione conformi ai principi di trattamento lecito e prevenzione del ischio introdotti dall'art. 6, n. 4 del nuovo regolamento UE n. 679/2016». Così G. GIANNONE CODIGLIONE, *I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la "consumerizzazione" della privacy*, in *Dir. inf*., 2/2017, 424.

[5] In argomento cfr. G. RESTA-Z. ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ*., 2/2018, 2, 411 ss.; G. D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Dir. inf. e informatica*, 4/2020, 635 ss. Sulla circolazione dei dati vedi R. MESSINETTI, *Circolazione dei dati personali e autonomia privata*, in *federalismi.it*, 3/2019; F. BRAVO, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contr. e impr*., 1/2019, 43; G. DI LORENZO, *La circolazione dei dati personali tra tutela della persona e ordine giuridico del mercato*, in *federalismi.it*, 21/2019, V. RICCIUTO, *La patrimonializzazione dei dati personali*, cit. 689 ss., nonché ID., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 23 ss., S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *Media-Laws – Riv. dir. media*, 3/2019, 131 ss., R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contr. e impr*., 2020,2, 760 ss. G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020. Peraltro, non sono rari i casi di contratti aventi ad oggetto beni personali. Basti pensare, ai contratti di sponsorizzazione (v. A. DE FRANCESCHI, *Il «pagamento» mediante dati personali*, in *I dati personali nel diritto europeo*, cit., 1384).

[6] Così G. D'IPPOLITO, *Monetizzazione, patrimonializzazione e trattamento di dati personali*, in AA.VV., *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, a cura di E. Cremona, F. Laviola e V. Pagnanelli, Torino, 2022, 55 s.

ISSN 2281-3918/2421-2563

immateriali e, segnatamente, attributi della persona di cui si può cedere l'utilizzazione economica a terzi (nel nostro caso le piattaforme social) [7] ma non la titolarità, che continua a restare nella sfera dominicale del loro originario titolare [8]. Lo "scambio" costituito dalla cessione, da parte dell'utente di servizi *social*, del diritto di sfruttamento economico dei dati personali dietro la fornitura, da parte del titolare del trattamento, di contenuti e/o servizi digitali ha dato luogo, in particolare, a due questioni non prive di conseguenze giuridiche: la sostanziale assimilazione della prestazione dei dati alla prestazione di denaro, quale controprestazione della fornitura di contenuti e servizi digitali forniti dalle piattaforme *online*, e la specificazione del ruolo che assume il consenso nei contratti di *social network*.

La prima questione ha trovato espresso riconoscimento in diversi interventi del legislatore europeo. Non solo la Direttiva UE n. 2161/2019, nel ridefinire la disciplina generale dei diritti dei consumatori, ha introdotto un comma 1-*bis* nell'art. 3 della Direttiva n. 83/2011 estendendone l'applicazione all'ipotesi in cui per l'accesso ai contenuti o servizi digitali il consumatore si impegna a fornire al professionista dati personali, ma anche la Direttiva UE n. 770/2019, nel disciplinare i contratti di fornitura di contenuti o di servizi digitali al considerando 24 e, soprattutto, all'art. 3, par. 1, ha previsto la sua applicazione anche all'ipotesi in cui la controprestazione del consumatore non è rappresentata dal pagamento di una somma di denaro ma dalla fornitura (anche sotto forma di impegno) dei dati personali (*recte* dall'attribuzione al professionista del diritto a trattare i propri dati personali).

Nonostante la formulazione più attenuata della norma rispetto a quella corrispondente della proposta di direttiva – che qualificava la fornitura di dati come controprestazione – non può negarsi che la sostanza del fenomeno sia rimasta immutata, lasciando molti dubbi, in dottrina, circa la sua ricostruzione in termini di contratto a prestazioni corrispettive [9], ricostruzione che, tenendo conto della natura

---

[7] Occorre evidenziare che la limitazione della circolazione dei dati personali derivante dalla loro assimilazione ai diritti della personalità appariva comunque eccessiva in quanto, com'è noto, non ogni disposizione negoziale dei diritti della personalità è, di per sé, illecita. Se lo sono sicuramente gli atti di disposizione a titolo oneroso che riguardano la persona nella sua corporeità, stante l'esistenza di un articolato impianto normativo, generale e speciale, che regola la materia degli atti dispositivi del corpo e li regola esclusivamente nell'alveo della gratuità (v. G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, 4-8), un discorso diverso, invece, va fatto per quel che concerne gli attributi immateriali (o astratti) della persona e, cioè, tutti quei caratteri che non rientrano nella sua sfera corporea, come l'immagine, il nome, la voce o i dati personali…). In queste ipotesi, infatti, non rinvenendosi alcuna normativa da cui poter dedurre il divieto di disporne a titolo oneroso da parte del titolare, non sembrano sussistere quei «limiti imposti dalla legge» all'autonomia privata, di cui all'art. 1322, comma 1, c.c. Assimilando agli attributi immateriali della persona i dati personali potrebbe, quindi, confermarsi che lo scambio di dati personali come controprestazione sarebbe astrattamente lecito. Tuttavia tale scambio, non integrando una vera e propria compravendita (perché manca l'effetto traslativo), deve essere verificato nella sua liceità e, quindi, per essere ammesso non dovrà contrastare con le norme imperative, l'ordine pubblico ed il buon costume. Così M. GIACCAGLIA, Facebook *è gratis? "Mercato" dei dati personali e giudice amministrativo*, in *Il diritto dell'economia*, 2/2020, 279.

[8] Non è un caso che anche chi sostiene la necessità di ammettere l'esistenza di un mercato di circolazione dei dati personali comunque li considera come attributi della persona e costitutivi della sua identità, con la conseguenza di escluderne la dismissione definitiva per atto del suo titolare (v. G. RESTA, *L'appropriazione dell'immateriale. Quali limiti?*, in *Dir. inf.*, 2004, 45). Interessanti considerazioni sulla possibilità di disporre degli attributi immateriali della persona in una logica diversa da quella proprietaria sono espresse da S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie personali al trattamento in massa dei dati personali*, Milano, 2018, 62 s. Ma vedi anche C. SOLINAS, *Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette*, in *Giur. it*., 2/2021, 325, per la quale se circolazione della ricchezza significa circolazione del diritto espressione di tale ricchezza, «non è certo il diritto fondamentale alla protezione dei dati personali che circola, né un diritto di stampo proprietario sui dati personali. Il contratto di circolazione del dato costituisce un diritto in capo al titolare del trattamento a godere dei benefici, diretti o indiretti, ricavabili dal trattamento del dato, in ragione proprio della peculiarità del dato personale che consente un godimento contemporaneo, ripetuto e spazialmente illimitato dello stesso».

[9] Secondo C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in *Giust. civ*., 3/2019, 505, la singolarità della defini-

ISSN 2281-3918/2421-2563

"bifronte" del dato ed adattando ad essa la disciplina applicabile (con conseguente esclusione di possibili effetti traslativi e definitivi o degli effetti vincolanti propri della disciplina contrattuale), ci sembra rimanga quella più accreditata in considerazione del fatto che la fornitura di contenuti e servizi digitali viene remunerata con (e, quindi, trova la sua causa giustificativa nel) la fornitura del diritto a trattare i dati personali dell'interessato ed a trarre da essi utilità.

Quanto al ruolo del consenso nei contratti di *social network*, come evidenziato da autorevole dottrina [10], occorre distinguere la volontà di richiedere la fornitura del servizio digitale o anche del bene – che si manifesta accedendo al sito e usufruendo di quanto dallo stesso offerto e che non presenta particolari problemi se non quelli propri di tutte le contrattazioni anche *off line* (la volontà contrattuale, per essere valida, non deve essere viziata né provenire da soggetti incapaci di agire) – dal consenso al trattamento dei dati, in virtù del quale la controparte professionale potrà trarre utilità economiche, la cui natura negoziale può desumersi dall'equiparazione, operata dalle più recenti normative europee a tutela dei consumatori, tra il contratto di fornitura di servizi digitali dietro pagamento di un corrispettivo da parte dell'interessato e l'operazione economica in cui quest'ultimo riceve i contenuti ed i servizi digitali obbligandosi (o impegnandosi) a fornire i propri dati personali, il cui trattamento non sarebbe necessario ai fini dell'esecuzione del contratto di *social network*, né per l'assolvimento, da parte del professionista, di obblighi di legge. Si registrano due importanti ricostruzioni in dottrina che assegnano, l'una, natura negoziale [11] e, l'altra, natura autorizzatoria [12] al consenso al trattamento dei dati per-

---

zione contenuta nell'art. 3 della Direttiva n. 770/2019 è data dal fatto che «le due *forniture* da parte dei due contraenti non sembrano poste in relazione formale di corrispettività, ragion per cui il contratto non si presenta né oneroso né a prestazioni corrispettive, bensì come "caso",…, in cui convergono la prestazione economica tecnicamente gratuita di contenuti o servizi digitali da parte dell'operatore economico, e in corrispondenza la fornitura di dati personali da parte del consumatore». Da qui la costruzione della fattispecie come fornitura contrattuale *a struttura gratuita* cui si affianca – *ma non in funzione corrispettiva* – un atto dispositivo mediante il quale il consumatore cede al fornitore i suoi dati personali, suscettibili di trattamento e verosimilmente trattati in relazione a scopi diversi da quelli contrattuali (altrimenti si tratterebbe di una fornitura *del tutto gratuita* e priva delle tutele consumeristiche in quanto il trattamento dei dati sarebbe necessario per l'esecuzione stessa del contratto) ed ottiene, per espressa previsione normativa, la stessa tutela prevista per il consumatore che paga per i servizi ricevuti (potrà esercitare i rimedi contro i difetti di conformità). Questi contratti rientrerebbero nel modello di *gratuità interessata*, e sarebbero caratterizzati da un doppio procedimento formale e da un *doppio consenso* da parte dell'utente del servizio: il primo, concernente la conclusione del contratto di fornitura (sottoposto alle ordinarie regole contrattuali) ed il secondo concernente la raccolta del consenso informato al trattamento dei dati e sottoposto alla disciplina del GDPR. Si tratterebbe, quindi, di due procedimenti negoziali autonomi ma tra loro collegati. Altra dottrina (V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ.*, 2020, 3, 652 s.), invece, al di là dello schema astratto utilizzato e della difficoltà di individuare un tipo contrattuale soprattutto nell'ipotesi in cui i dati personali vengono forniti senza ricevere un corrispettivo in denaro, ritiene che anche in questi schemi, dove la fornitura di dati è solo apparentemente gratuita, venga in gioco una causa di scambio. Per l'A. la causa concreta del contratto «consente di rinvenire nella prestazione avente ad oggetto i dati personali il corrispettivo dei beni e dei servizi digitali. E questo nonostante la formulazione dell'art. 3, Dir. n. 770/2019 che ha volutamente evitato di far riferimento al termine «corrispettivo» su parere del Garante europeo per la protezione dei dati personali (v. *EDPS*, *Opinion 4/20178*, in *www.edps.europa.eu*). Quest'ultimo, pur riconoscendo l'esistenza di un mercato europeo dei dati personali, riteneva «pericoloso» accostare concettualmente e testualmente alla controprestazione pecuniaria quella costituita dalla fornitura di dati in quanto la protezione dei dati personali è un diritto fondamentale insuscettibile di essere considerato in termini di mera «merce» e, quindi, di corrispettivo.

[10] Il riferimento è ad A. GENTILI, *La volontà nel contesto digitale: interessi del mercato e diritti delle persone*, in *Riv. trim. dir. proc. civ.*, 3/2022, 709 ss.

[11] Vedi, tra gli altri, G. RESTA-V. ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2/2018, 434.

[12] Si tratta della tesi di F. BRAVO, *Lo "scambio di dati personali"*, cit., 43 ss., che richiama la distinzione formulata da A. AURICCHIO (voce *Autorizzazione*, in *Enc. dir.*, Milano IV, 1959, par. 2), tra autorizzazione "integrativa" (cui è ricollegabile il consenso – condizione di liceità del trattamento dei dati personali), dall'autorizzazione "costitutiva", in quanto la prima, pur

ISSN 2281-3918/2421-2563

sonali. Tali ricostruzioni, sebbene poste come divergenti, potrebbero essere combinate [13] in considerazione del fatto che anche il trattamento dei dati è, per così dire, *duplice* [14]. Si registra, infatti, un trattamento «necessario alla fornitura del servizio e nei confronti del quale le norme sulla protezione dei dati personali mirano a proteggere la riservatezza, l'identità e la personalità degli interessati», ed un trattamento necessario, invece, a remunerare il titolare della sua attività. Il consenso relativo al primo ha sicuramente natura autorizzatoria (rimuovendo «un ostacolo o un limite al potere o alla facoltà che l'ordinamento già accorda al titolare del trattamento, in funzione del perseguimento di propri interessi, lecitamente perseguiti» [15]), mentre, con riferimento al secondo trattamento, il consenso non può che avere natura negoziale (in quanto permette al titolare del trattamento di svolgere la propria attività economica e di fare guadagni), per cui la tutela dell'utente qui è vista nell'ottica di garantire *un'equità dello scambio* rispetto ad un'operazione economica caratterizzata da una forte asimmetria informativa nei suoi confronti [16] e congegnata alla stessa stregua dei contratti per adesione, dove l'aderente (nel nostro caso l'utente) potrà solo "prendere" (acconsentire anche al trattamento di dati personali non strettamente necessari per ottenere i servizi social) o "lasciare" (decidere di rinunciare ai servizi social) [17]. Poiché lo "scambio" servizi contro dati è funzionale a realizzare quello che è stato definito, da

essendo un istituto privatistico condividerebbe con l'autorizzazione amministrativa il fine di rimuovere un limite all'esercizio di un potere o di una facoltà.

[13] Vedi anche le osservazioni di A. GENTILI, *op. cit*., 713 s.

[14] Cfr. G. D'IPPOLITO, *Commercializzazione dei dati personali*, cit., 659.

[15] Così F. BRAVO, *Lo "scambio di dati personali"*, cit., 43 s. per il quale il consenso ha carattere autorizzatorio e preventivo, costituendo un atto «prodromico rispetto all'attività giuridica del titolare del trattamento». Peraltro, l'A. evidenzia proprio come questa impostazione non è preclusiva rispetto alla possibilità di "*commercializzazione*" dei dati personali che vanno, però, inquadrate diversamente, sotto il profilo giuridico, ammettendo un consenso contrattuale ontologicamente distinto, sebbene collegato, a quello reso in materia di protezione dei dati personali.

[16] Evidenzia A. GENTILI, *op. cit.*, 701 ss. come dalla stessa normativa del GDPR emerga la disparità di potere negoziale delle due parti e la legittimazione legale del mercato dei dati «con pochi, fiacchi e platonici limiti a protezione della persona». Ciò deriverebbe anche dalla circostanza che nella disciplina in questione il fondamento della legittimazione a trattare dati non è il consenso dell'interessato ma «la libertà di circolazione dei dati e in generale il principio capitalistico sotteso al mercato. Sono i fornitori dei servizi digitali che nei *Terms of service* stabiliscono le condizioni per l'erogazione. E nella quasi totalità dei casi il consenso ha un ruolo marginale, limitato ai servizi accessori». Ciò è confermato anche dalla possibilità riconosciuta ai titolari del trattamento di giustificare la raccolta e l'utilizzo dei dati personali non realmente necessari per l'erogazione del servizio quando ciò corrisponda ad un "legittimo interesse" dei medesimi. Per l'A. se il legislatore avesse voluto bilanciare l'interesse dell'impresa con quello degli utenti «avrebbe dovuto instaurare il controllo del trattamento dati attraverso specifiche disposizioni di legge» così come ha fatto in materia consumeristica, e comunque ad un vero bilanciamento si sarebbe potuti giungere impostando siti di navigazione in modo tale che gli utenti dovessero dare il consenso a tutti i *cookie* non strettamente necessari all'erogazione del servizio, piuttosto che trovarsi già un consenso presunto e doversi attivare per rifiutarlo.

[17] Sulla duplicità dei consensi dissentono, invece, V. RICCIUTO, *Consenso al trattamento e contratto*, in S. ORLANDO (a cura di), *Libertà e liceità del consenso nel trattamento dei dati personali*, in *Pers. merc.*, Firenze, 2024, 31 ss., e S. ORLANDO, *Il coordinamento tra la Direttiva 2019/770 e il GDPR. L'interessato consumatore*, in *Pers. merc*., 2/2023, 231. In particolare il primo evidenzia come «ricostruire una vicenda circolatoria di carattere patrimoniale, quale quella relativa all'ipotesi di scambio dei dati personali, che muove dall'idea che ogni decisione di un soggetto in ordine ai propri dati personali debba esaurirsi nel (limitato) orizzonte della c.d. autodeterminazione informativa, alla quale, sulla scia dell'esperienza tedesca, si è fatto riferimento in sede di interpretazione della l. n. 675/199613. Il contesto nel quale tali originarie posizioni trovavano un qualche fondamento è però del tutto modificato da un punto di vista, intanto, normativo (con le modifiche alla originaria disciplina della l. n. 675/1996, la quale del tutto marginalmente si preoccupava delle vicende circolatorie); dalle letture che gli interpreti hanno successivamente offerto del fenomeno e, ancora di più, dall'erompere del fenomeno del trattamento dei dati nelle attività economiche e che ha portato all'adozione del Regolamento il quale, invece, offre (certo non esclusivamente) gli strumenti per una ricostruzione in chiave pienamente patrimonialistica e negoziale».

ISSN 2281-3918/2421-2563

più parti, come capitalismo della "sorveglianza" [18], occorre esaminare più da vicino il *business* model di cui lo stesso si serve per realizzare i suoi obiettivi (ovvero captare le scelte degli utenti per poi poterle indirizzare e, addirittura, manipolare).

2. – Nella prassi di mercato dei *social network* il modello di *business* probabilmente più diffuso è rappresentato dal trattamento e dalla circolazione dei dati quale corrispettivo dei diversi servizi offerti. Rispetto al passato, infatti, la fornitura del dato non è più un elemento strumentale all'attività dell'impresa, ma diventa la ragione principale del suo svolgimento. I dati costituiscono, cioè, la base del *business* imprenditoriale per le potenzialità di ricchezza connesse alla loro aggregazione, analisi, profilazione ecc. [19], tutte attività che l'impresa svolge servendosi degli algoritmi e dell'IA. Si parla, nello specifico, di modello di business "*zero-price*" volendo così rappresentare la circostanza che, in queste economie, i servizi digitali vengono offerti all'utente "gratuitamente", o meglio senza che lo stesso debba eseguire una controprestazione di natura pecuniaria perché gli basterà acconsentire al trattamento dei propri dati personali per la realizzazione di interessi commerciali [20].

Questo modello si distingue dall'ipotesi in cui lo scambio dei dati avviene, invece, contro moneta (c.d. *personal data economy model*), nel senso che agli utenti viene riconosciuta una parte o l'intero valore che ai dati è attribuito dalle piattaforme mediante i processi di profilazione e *adversiting*. Poiché alla fornitura del dato da parte dell'utente segue la corresponsione di una somma di denaro, si parla di "monetizzazione" dei dati personali, sebbene in dottrina si escluda che anche nel modello di monetizzazione possa verificarsi una sorta di equiparazione tra dati personali e moneta. Lo impedisce il dettato dell'art. 3, par. 1, direttiva 2019/770 «che prevede che i dati siano utilizzati direttamente per accedere a beni e servizi, non anche per la remunerazione dell'utente».

Si tratta di diversi modelli di "commercializzazione" dei dati personali, non sempre facilmente distinguibili nella pratica, e rispetto ai quali le garanzie a tutela di chi fornisce i dati sono differenti. Lasciando da parte il modello in cui si assiste, comunque, ad una remunerazione in denaro della fornitura del dato personale ed approfondendo, invece, le caratteristiche del modello "*zero price*", occorre ancora distinguere diversi livelli di patrimonializzazione dei dati. A livello più basso troviamo l'ipotesi dei dati forniti dall'utente in quanto necessari alla stessa esecuzione del servizio da parte del fornitore. Qui non si può parlare propriamente di "commercializzazione" dei dati personali perché qui la fornitura del dato non è, economicamente considerata come un'alternativa al denaro, ma si giustifica quale condizione fattuale perché il titolare del trattamento possa eseguire un comportamento obbligatoriamente (già) dovuto in base ad un contratto o alla legge, tanto che il trattamento viene subordinato al rispetto delle sole regole del GDPR [21].

---

[18] Su cui vedi, tra gli altri, S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, II ed., Roma, 2023, *passim*; G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020, in part. capitolo 1, e A. QUARTA, *Mercati senza scambi. Le metamorfosi del contratto nel capitalismo della sorveglianza*, Napoli, 2020.

[19] Proprio in considerazione della ingente massa di dati diversi per oggetto e per soggetto disponibili nell'ecosistema digitale, prodotti ad alta velocità e derivanti da fonti altamente differenziate, gestiti ed analizzati da sempre nuovi e più avanzati algoritmi, non si parla più di semplici dati ma di "big data". Sul tema, *amplie*, A. DI LANDRO, *Big Data. Rischi e tutele nel trattamento dei dati personali*, Napoli, 2020; G. D'ACQUISTO-M. NALDI, *Big Data e Privacy by design. Anonimizzazione Pseudonimizzazione Sicurezza*, Torino, 2017.

[20] Sul punto G. D'IPPOLITO, *Monetizzazione, patrimonializzazione e trattamento di dati personali*, 58 s. Con riferimento al trattamento dei dati personali per finalità di marketing online diffusamente ID., *Profilazione e pubblicità targhettizzata online. Real-Time Bidding e behavioural adversiting*, Napoli, 2021.

[21] Non opereranno, invece, le norme e le tutele relative alla concessione/vendita dei dati, incluse quelle contenute nella Direttiva 2019/770/UE (vedi art. 3, par. 1).

ISSN 2281-3918/2421-2563

Ad un livello superiore si colloca, invece, l'ipotesi in cui il fornitore dei servizi digitali richieda dati ulteriori rispetto a quelli necessari alla fornitura del servizio, perché qui la *commercializzazione* dei dati personali non è dubitabile. Si tratterà di assicurare che il trattamento di questi dati "altri" rispetto a quelli necessari all'esecuzione del servizio avvenga nel rispetto dei principi di liceità, limitazione delle finalità e minimizzazione previsti dal GDPR. Di conseguenza il titolare del trattamento dei dati dovrà informare effettivamente e adeguatamente l'interessato delle finalità diverse che si intendono perseguire affinché l'interessato potrà essere messo al corrente dei trattamenti ulteriori (e magari non voluti) e ciò anche al fine di non veder qualificata la propria condotta come pratica commerciale scorretta con le conseguenze giuridiche che ne deriverebbero.

Ma un livello ancora più sofisticato (e forse più diffuso) di patrimonializzazione dei dati si ha quando il fornitore del servizio digitale condiziona la fornitura di un servizio richiesto dall'utente al consenso prestato dallo stesso al trattamento dei suoi dati per servizi a lui non necessari ma da cui il titolare del trattamento può ottenere remunerazione (es. l'invio di newsletter per finalità di marketing). Si tratta del fenomeno del "tying" [22] o "bundling" dove si assiste ad una condizionalità che non è espressione di un consenso liberamente prestato [23]. Detto altrimenti, se l'utente negherà il consenso al trattamento per usufruire del servizio accessorio non potrà più usufruire neppure del servizio principale. Occorre allora capire se i servizi sono tra loro collegati, ma autonomi (per cui non opererà l'art. 7 GDPR), oppure se esiste una condizionalità perché, in quest'ultimo caso, la condizionalità sarà lecita solo se basata su un consenso "liberamente prestato". Su questo punto si sono formati due orientamenti: uno più rigoroso e l'altro più liberale. Il primo, partendo dall'assunto che il consenso dell'interessato sia elemento non negoziabile delle condizioni generali di contratto (o di servizio) unilateralmente predisposte dal professionista, ritiene lecita la condizionalità soltanto nel caso in cui il titolare offra all'interessato la scelta tra un servizio condizionato all'uso dei dati personali per finalità supplementari e lo stesso servizio "equivalente" che però non richieda un siffatto consenso.

Il secondo orientamento, invece, recepito dalla nostra S.C. nella pronuncia n. 17278/2018 [24], am-

---

[22] Evidenzia G. D'IPPOLITO, *Monetizzazione, patrimonializzazione e trattamento di dati personali*, cit., 68 come la fattispecie del *tying*, quale peculiare condizione a cui viene subordinata l'esecuzione del contratto, «è quella dietro la quale è più probabile che si annidi un fenomeno di commercializzazione e patrimonializzazione dei dati personali,

nonché, forse, quello che più si avvicina all'uso dei dati personali quale nuova *currency*, in quanto solo in questo caso l'utente non potrà accedere al servizio senza aver ceduto dati per finalità da lui non richieste, non necessari al servizio ma che soddisfano il solo interesse del titolare ad ottenere profitti.».

[23] Le condizioni del consenso sono indicate all'art. 7 GDPR dove si prevede che nelle ipotesi di trattamento basate sul consenso il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali e soprattutto, al par. 4 si stabilisce che «Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto». La norma va letta unitamente al considerando 43 del GDPR dove si prevede una presunzione di consenso non libero e quindi invalido nel caso in cui «non è possibile prestare un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione». Sulla libertà del consenso e sull'interpretazione dell'art. 7, comma 4, GDPR v'è chi (C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, 96) ritiene che la norma rappresenti il riconoscimento e non la negazione della possibilità di scambiare liberamente il consenso al trattamento dei dati non necessari all'esecuzione del contratto con la fornitura dei servizi digitali.

[24] In *Giur. it*., 2019, 3, con commento di S. THOBANI, *Operazioni di* tying *e libertà del consenso*. Nel caso di specie la S.C., pur accogliendo il ricorso del Garante per mancanza di specificità del consenso, si discosta dal rigore della sua interpretazione ritenendo che il consenso può considerarsi libero anche quando una prestazione sia ad esso condizionata purché si

ISSN 2281-3918/2421-2563

mette la possibilità di condizionare il contratto alla prestazione del consenso al trattamento dei dati per altre finalità (es. l'invio di comunicazioni commerciali da parte di terzi) nel caso in cui il servizio principale sia "fungibile", nel senso che sia uno dei tanti servizi disponibili sul mercato a cui l'utente possa rinunciare senza gravoso sacrificio. Tra queste posizioni, per così dire "estreme", una via di mezzo potrebbe essere rappresentata dal considerare lecita una condizionalità necessaria di cui il consumatore venga, però, effettivamente ed adeguatamente informato prima di effettuare la sua scelta commerciale, anche per escludere la qualificazione della pratica commerciale posta in essere dal fornitore dei servizi 'combinati' come scorretta perché ingannevole o aggressiva [25].

3. – A fondamento delle decisioni dell'AGCM ora in esame vi è l'acquisizione che i dati personali siano caratterizzati da una duplice dimensione, personale e patrimoniale. Proprio per quest'ultima componente, necessaria allo sviluppo dei mercati digitali, non è più "in forse" la patrimonializzazione/commercializzazione dei dati personali ma è necessario, per un verso, assicurare che le operazioni economiche [26] aventi ad oggetto il loro sfruttamento a fini commerciali non contrastino con la normativa sulla c.d. *data protection* e, per altro verso, accettare l'idea che i contratti di "cessione" dei dati personali non possano essere traslativi della proprietà, come accade per qualunque altro bene negoziabile, «non essendo una definitiva perdita del diritto in parola compatibile con la sua natura di diritto fondamentale» [27]. La circostanza, poi, che vi sia un legame corrispettivo tra il servizio di accesso al *social network* e la prestazione del consenso al trattamento dei (propri) dati personali (da parte) dell'utente, oltre ad orientare verso la natura negoziale del consenso [28] assegna ad esso il ruolo di pa-

---

tratti di un condizionamento "controllato" nel senso che, per un verso, il consenso non deve essere viziato dai vizi della volontà né da "possibili disorientamenti, stratagemmi, opacità, sotterfugi, slealtà, doppiezze o malizie comunque adottate dal titolare del trattamento"; e, per altro verso, la prestazione condizionata dalla prestazione del consenso al trattamento non dev'essere "infungibile ed irrinunciabile per l'interessato". Per un approfondimento sull'interpretazione del requisito della libertà del consenso v. ancora S. THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. dir. priv.*, 2/2016, 513 ss.

[25] In quest'ultimo senso si è pronunciata ad es. L'AGCM – PS 10207 – *Promozioni scorrette, sanzioni a Samsung Electronics Italia* per oltre tre milioni di euro del 25 gennaio 2017.

[26] Diverse sono le incertezze che concernono le qualificazioni contrattuali di queste operazioni economiche tanto che qualche autore (P. GALLO, *Il consenso al trattamento dei dati personali come prestazione*, in *Riv. dir. civ.*, 6/2022, 1064 s.) ipotizza un contratto *a causa mista*, assimilabile alla commercializzazione del diritto patrimoniale d'autore o allo sfruttamento economico dell'immagine, dove però la controprestazione non è rappresentata da un corrispettivo monetario ma dal consenso al trattamento dei dati personali, peraltro revocabile *ad nutum*.

[27] Così B. PARENZO, *Dati personali come "moneta". Note a margine della sentenza TAR Lazio n. 260/2020*, in questa *Rivista*, 5/2020, 1372.

[28] Quello della natura giuridica del consenso è un profilo controverso in dottrina. Parte di essa, infatti, valorizzando la natura patrimoniale del dato, considera il consenso come un vero e proprio atto di disposizione compiuto dall'interessato del trattamento sui suoi beni (i dati personali) facenti parte del proprio patrimonio (vedi, per tutti, G. OPPO, *"Trattamento" dei dati personali e consenso dell'interessato*, in ID., *Scritti giuridici*, VI, *Principi e problemi del diritto privato*, Padova, 2000, 113 e V. CUFFARO, *A proposito del consenso*, in V. CUFFARO-V. RICCIUTO-V. ZENO ZENCOVICH, *Trattamento dei dati e tutela della persona*, Milano, 1999, 121). Altri autori, invece, propendono per una ricostruzione del consenso al trattamento dei dati personali come atto giuridico in senso stretto, di tipo scriminante (è la posizione di S. PATTI, *Commento all'art. 23*, in *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 ("Codice della privacy")*, a cura di C.M. Bianca, F.D. Busnelli, Padova, 2007, 553, e di I. CAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *ODCC*, 2018, 84 s.) o di tipo autorizzatorio (cfr., tra gli altri, F. BRAVO, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, cit., 34, nonché, ID., *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Padova, 2018, 107 ss. e D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, 354).

ISSN 2281-3918/2421-2563

rametro della liceità della controprestazione, nel senso che il trattamento dei dati cui si acconsente sarà lecito solo se, e fintanto che, si svolga per le finalità che sono state indicate al concedente e non per altre [29]. Con la conseguenza, sotto il profilo contrattuale, che l'utilizzo dei dati per finalità diverse da quelle dichiarate, può, con il concorso di altre circostanze, costituire una pratica commerciale scorretta o, comunque, una condotta anti-consumeristica. Tra le vicende che hanno suscitato particolare interesse ai fini della qualificazione dell'illecito trattamento dei dati personali come pratica commerciale scorretta un ruolo significativo è assunto dai casi *Facebook* del 2018 e *Meta* del 2024. Il primo di essi ha visto contrapposti il noto colosso dei servizi *social* (*Facebook Ireand Ltd.*, appunto, società europea controllata dall'americana *Facebook Inc*.) e l'AGCM per la presunta violazione, da parte della piattaforma digitale, di alcune regole del codice del consumo (gli artt. 20, 21, 22, 24 e 25 concernenti le pratiche commerciali ingannevoli ed aggressive). In questa occasione l'AGCM ha riconosciuto la scorrettezza di due pratiche e, precisamente, ha considerato ingannevole la condotta del professionista che non aveva informato adeguatamente e immediatamente l'utente, in fase di attivazione dell'*account*, dell'attività di raccolta e utilizzo per finalità informative e/o commerciali dei dati che l'utente gli aveva ceduto (dichiarando, anzi, la gratuita fruizione del servizio e inducendolo, così, ad assumere una decisione di natura commerciale – quella di registrarsi a Facebook – che altrimenti non avrebbe preso), e aggressiva la condotta di Facebook per avere indebitamente condizionato i consumatori registrati, in cambio del servizio social, a consentire a Facebook medesimo ed a terzi la raccolta e l'utilizzo dei loro dati, in modo inconsapevole e automatico, prevedendo, in caso di deselezione delle informazioni, penetranti limitazioni nell'utilizzo della piattaforma social [30]. Il provvedimento dell'AGCM è stato parzialmente accolto dalla giurisprudenza amministrativa, prima del TAR Lazio [31], e successivamente del Consiglio di Stato che ha confermato la sentenza di primo grado [32].

La difesa di Facebook si incentrava, essenzialmente, sulla mancanza di legittimazione dell'AGCM a sanzionarla, non essendoci pratiche commerciali da vagliare per la mancanza di qualsiasi corrispettivo patrimoniale da parte dei consumatori. Questi ultimi, secondo la ricorrente, non avrebbero potuto mai cedere i propri dati come corrispettivo di una prestazione, essendo la gestione dei dati personali un'attività a carattere non patrimoniale ove non è coinvolto l'interesse economico del singolo utente e,

[29] Ciò almeno tutte le volte in cui non sia l'ordinamento a prevedere condizioni di liceità del trattamento diverse dal consenso.

[30] Nella pronuncia dell'AGCM si è evidenziato che le versioni del sito web di Facebook anteriore e successiva al 15 aprile 2018 si basavano comunque su meccanismi di *opt-out*. E qualora l'utente fosse approdato alle schermate relative all'opzione sarebbe stato, in ogni caso, disincentivato dal modificare la selezione preimpostata da Facebook a causa del carattere fortemente penalizzante delle limitazioni previste (nella fruizione del social network, di siti web e app di terzi) e rappresentate da espressioni del tipo: "non potrai accedere ai siti Web o alle app usando Facebook", "non sarai in grado di accedere ai giochi o alle applicazioni mobili usando Facebook", "i tuoi amici non potranno interagire con te e condividere elementi usando le app e i siti web", "verrà disattivata anche la personalizzazione istantanea", "le app a cui hai effettuato l'accesso (tramite Facebook o in modo anonimo) saranno rimosse", "i post delle app saranno rimossi dal tuo profilo".

[31] Si tratta di TAR Lazio, 10 gennaio 2020, n. 260, in questa *Rivista*, 5/2020, 1355 ss.

[32] Il riferimento è a Cons. Stato, 29 marzo 2021, n. 2361, in *Nuova giur. civ. comm.*, 2021, con nota di D. D'ALBERTI, *Tutele "multilivello" e l'effettività dei rimedi per gli utenti online* (dove si approfondisce anche il problema della c.d. *parental liability*, ovvero della responsabilità della società controllante per gli illeciti compiuti dalla sua controllata); in *Resp. civ. prev*., 5/2021, 1604 ss., con nota di L. CASALINI, *Dati personali all'inserzione tra diritto del consumo e tutela della privacy*; in *giustiziacivile.com*, con nota di V. RICCIUTO-C. SOLINAS, *Fornitura di servizi digitali e prestazione di dati personali: punti fermi ed ambiguità sulla corrispettività del contratto*, in *Foro it.*, 2021, 325 ss., con nota di A. D'AVOLA-R. PARDOLESI, *Protezione dei dati personali, tutela della concorrenza e del consumatore (alle prese con i "dark pattern"): parallele convergenti?*

ISSN 2281-3918/2421-2563

di conseguenza, non potendosi applicare al caso da decidere la disciplina consumeristica l'unica normativa applicabile sarebbe stata quella relativa alla protezione dei dati personali.

Su questo punto il Consiglio di Stato (richiamando la pronuncia del TAR) chiarisce che le due discipline, *privacy* e consumeristica, sono complementari ed esclude che l'omessa informazione sullo sfruttamento dei dati dell'utente a fini commerciali sia una questione disciplinata esclusivamente dal *General Data Protection Regulation* (da ora GDPR o RGDP) [33]. Ma, soprattutto, propone il cumulo dei rimedi per offrire una tutela *multilivello* dei diritti delle persone fisiche, anche quando un diritto personalissimo sia sfruttato a fini commerciali [34]. Peraltro, la disciplina consumeristica (e segnatamente quella sulle pratiche commerciali scorrette) si rivelava particolarmente idonea a garantire una tutela effettiva dell'utente/consumatore, sia per la gamma di comportamenti colpiti, indipendentemente dall'esistenza di un rapporto negoziale, sia per la natura di illecito di pericolo che caratterizza le pratiche commerciali scorrette (per cui rileva la potenzialità lesiva della condotta e non anche l'effettiva lesione della autodeterminazione dell'utente). Senza contare la "velocità" della tutela amministrativa da parte dell'AGCM e la circostanza che la stessa sia rivolta non solo al singolo consumatore ma alla collettività dei consumatori.

L'assunto da cui era partita *Facebook* (ovvero l'idea che i dati personali non possono essere considerati merce in quanto costituiscono beni *extra commercium*, trattandosi di diritti fondamentali della persona) viene, quindi, superato dal Consiglio di Stato che sposta l'attenzione dal dato personale alla sua protezione e considera proprio tale protezione come diritto fondamentale, come diritto all'*autodeterminazione informativa*.

Ogni individuo, in altri termini, ha diritto di controllare e gestire il proprio patrimonio informativo, di decidere sui propri dati. Non a caso il GDPR fornisce ai singoli specifici strumenti di tutela che vanno dal diritto di limitazione con cui si riduce l'attività di trattamento del titolare alla mera conservazione dei dati, al diritto di opposizione dell'interessato ai trattamenti posti in essere per motivi di interesse pubblico (compresi i trattamenti di profilazione), al diritto di revocare il consenso prestato in qualunque momento e con la stessa facilità con cui è stato accordato.

Si conferma, quindi, che è la stessa disciplina del GDPR a garantire all'interessato la possibilità di disporre dei propri dati attraverso lo strumento del consenso che presuppone un'informazione trasparente e chiara rispetto ad ogni trattamento che riguardi i suoi dati personali [35], ma non contempla divieti espliciti relativi alla commercializzazione dei dati, attività che rappresenta, come detto poc'anzi, il *business model* delle piattaforme social [36]. L'impiego dei dati personali per attività di profilazione con-

---

[33] Peraltro, al fine di escludere la sovrapponibilità dei piani relativi alla tutela della "privacy" e alla protezione del consumatore i giudici amministrativi richiamano la decisione della CGUE 13 settembre 2018, cause riunite C-54/17 e C-55/17, *AGCM contro Wind Tre SpA e Agcm contro Vodafone Itala SpA*, dove si è affermato il principio che in caso di conflitto tra le disposizioni della direttiva sulle pratiche commerciali sleali ed altre norme dell'Unione, che disciplinano aspetti specifici sempre delle pratiche commerciali sleali, queste altre norme prevalgono e si applicano a tali aspetti specifici. In dottrina cfr. M. MIDIRI, *Privacy e antitrust: una risposta ordinamentale ai Tech Giant*, in *federalismi.it*, del 13 maggio 2020, 227 s.

[34] Sul punto, in dottrina, F. LAVIOLA, *Il diritto all'autodeterminazione informatica tra concorrenza e* data protection, in AA.VV., *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, a cura di E. Cremona, F. Laviola e V. Pagnanelli, Torino, 2022, 45.

[35] Il considerando 39 del GDPR specifica, infatti, che dovrebbero essere trasparenti le modalità con cui i dati personali sono raccolti, utilizzati, consultati o altrimenti trattati, in particolare per quanto attiene alle finalità del trattamento, e che gli interessati dovrebbero essere sensibilizzati rispetto ai rischi del trattamento e alle modalità di esercizio dei loro diritti.

[36] Al par. 8 della pronuncia si afferma, infatti che «la patrimonializzazione del dato personale … costituisce il frutto dell'intervento delle società attraverso la messa a disposizione del dato – e della profilazione dell'utente – a fini commerciali».

ISSN 2281-3918/2421-2563

sente ai *Social* di fornire (dietro corrispettivo) i risultati del *targeting* a soggetti terzi (che sono i veri clienti delle piattaforme digitali), che li utilizzeranno a fini commerciali per effettuare pubblicità mirate [37]. Occorre precisare che nel caso deciso non veniva in rilievo la violazione, da parte di *Facebook*, degli obblighi di trasparenza e di informazione posti dal GDPR (in quanto Facebook, nelle condizioni d'uso della piattaforma, aveva comunicato agli utenti che i loro dati sarebbero stati impiegati per ricevere una pubblicità personalizzata e che, quindi, sarebbero stati forniti in forma anonima a terzi inserzionisti che, grazie all'attività di profilazione, avrebbero potuto proporre inserzioni che avrebbero incrociato gli interessi e i gusti dei destinatari), quanto la disciplina sulle pratiche commerciali scorrette, avendo il colosso americano ingannato gli interessati facendo loro credere che il servizio *social* fosse gratuito e, quindi, per aver omesso di fornire agli interessati un'informazione completa e trasparente sull'utilizzo a fini commerciali dei loro dati [38].

Proprio la qualificazione (fatta dall'AGCM e dai giudici) del contratto di iscrizione a *Facebook* come oneroso e non gratuito ha rappresentato la premessa per poter giungere ad affermare la responsabilità in ordine alle condotte tenute da *Facebook* come pratiche commerciali scorrette. Se, viceversa, fossero state ritenute fondate le censure di *Facebook* relative all'assenza di qualsivoglia corrispettivo a carico dell'utente per l'utilizzo del servizio, l'unica disciplina applicabile sarebbe stata quella sulla *privacy* e, conseguentemente, le relative sanzioni avrebbero potuto essere irrogate solo dal Garante privacy [39].

Qualche anno più tardi l'AGCM è stata chiamata a pronunciarsi su due pratiche commerciali "in

---

[37] Sulla pubblicità mirata cfr., per tutti, F. GALLI, *La pubblicità mirata al tempo dell'intelligenza artificiale: quali regole a tutela dei consumatori?*, in *Contr. e impr.*, 2/2022, 919 ss. il quale mette in guardia sui problemi che ne derivano per i consumatori che sono indebitamente influenzati da forme di pubblicità sempre più pervasive. Le pratiche di pubblicità mirata possono limitare l'autonomia decisionale dei consumatori e manipolarli. La pubblicità mirata può anche dar vita a trattamenti differenziati e discriminatori nel senso di rendere l'accesso a beni e servizi più svantaggioso per alcuni individui e categorie di consumatori rispetto agli altri. Così alcune categorie di persone possono essere sistematicamente escluse da certe opportunità di mercato, in base a valutazioni automatiche individualizzate e senza una logica accettabile. Senza contare che i problemi legati alla pubblicità mirata possono riguardare anche ambiti diversi da quello commerciale. Le tecniche manipolatorie, infatti, possono essere impiegate oltre che per orientare le scelte di consumo anche per orientare le opinioni ed i comportamenti politici dei cittadini, con pregiudizio per le democrazie. Al fine di arginare il fenomeno e, soprattutto, il nuovo squilibrio informativo che caratterizza i rapporti tra i commercianti ed i consumatori (vedi L. AMMANNATI, *La circolazione dei dati: dal consumo alla produzione*, in *Riv. trim. dir. econ.*, 2020, 4, 663), sono intervenute sia le norme del GDPR sulla profilazione e sulle decisioni automatizzate (vedi *anche Le Linee Guida Sul Processo Decisionale Automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/679* adottate dal Gruppo di Lavoro Articolo 29 il 3 ottobre 2017, 16 e 17, con le successive modifiche), sia la Direttiva 2161/2019/UE (che ha introdotto nuovi requisiti di trasparenza rilevanti per la pubblicità mirata). Nuovi obblighi informativi sono stati poi previsti dalle modifiche introdotte alla direttiva sui diritti dei consumatori del 2011 (art. 6-*bis* (1) (a)) ed a quella sulle pratiche commerciali sleali (art. 7 (4 a)), nonché dal *Digital Services Act* (DSA).

[38] Occorre evidenziare che, successivamente, con due sentenze "gemelle" del 18.11.2022 il TAR Lazio, è tornato ad occuparsi di pratiche commerciali sleali e patrimonializzazione di dati personali e si è pronunciato, con esiti opposti, sulle impugnative proposte da *Apple* e *Google* avverso provvedimenti emessi nei loro confronti dall'AGCM.

[39] Sul punto vedi anche C. SOLINAS, *Circolazione dei dati personali*, cit., 322 dove si afferma che la posizione della società ricorrente esprimeva l'idea per cui il trattamento dei dati personali poteva trovare collocazione nell'ambito della sola tutela della persona e non anche in quello dei rapporti patrimoniali e della loro disciplina generale. Da qui anche l'ulteriore motivo di ricorso per cui Facebook contestava la violazione del principio di legalità/prevedibilità, in quanto sarebbe stata sanzionata "sulla base di una disciplina (quella sulle pratiche commerciali scorrette) la cui applicazione era imprevedibile e nuova", ed in virtù della quale sarebbero state applicate, con dubbia legittimità, "sanzioni sulle pratiche commerciali al diverso tema della gestione dei dati personali e comunque a pratiche in cui non viene in questione un interesse economico diretto del consumatore".

ISSN 2281-3918/2421-2563

odore di scorrettezza" poste in essere da *Meta Platforms Ireland*[40]: la prima, similmente al caso *Facebook*, consisteva nella presunta ingannevolezza della condotta di *Meta Platform Ireland Ltd* e della sua controllante americana *Meta Platform Inc.* per aver omesso di informare gli utenti della piattaforma *Instagram*, all'atto della attivazione e prima registrazione dell'*account*, dell'attività di raccolta e di utilizzo, per finalità commerciali, dei dati dell'utente, così da indurlo ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso (ovvero l'utilizzo della piattaforma al "prezzo" dei propri dati); la seconda pratica (anch'essa ingannevole) si articolava, invece, nella mancata comunicazione agli utenti già registrati di un'adeguata motivazione in merito alla decisione da parte dei *social network Facebook* ed *Instagram* di sospendere l'utilizzo dell'*account* di un utente, limitando poi di molto il contraddittorio sulle richieste di revisione della decisione e nell'assenza di un'assistenza idonea nei casi in cui l'utente doveva recuperare un account a cui non poteva più accedere. A seguito dell'istruttoria condotta dall'AGCM è emersa la scorrettezza di entrambe le pratiche, nel primo caso per violazione degli artt. 20, 21, e 22 cod. cons. [41] e nel secondo caso dell'art. 20 cod. cons. [42], con la previsione di una sanzione amministrativa pecuniaria complessiva, per entrambe le infrazioni, di 3.500.000 euro. Merita attenzione, innanzitutto, il profilo relativo alla competenza dell'AGCM, contestata dalla Piattaforma social. Secondo Meta, infatti, il Garante avrebbe violato diversi principi europei: il principio del Paese di origine, quello della *lex specialis* e la primazia del diritto dell'Unione europea. In particolare, l'AGCM non avrebbe potuto applicare provvedimenti contrastanti con il quadro giuridico esistente (GDPR, Direttiva *e*-privacy, Direttiva *E-Commerce*, regolamento (UE) 2022/2065 sul Mercato Unico dei Servizi Digitali, "DSA") o imporre obblighi o ulteriori requisiti specifici diversi da quelli tipizzati dal legislatore europeo, per non vanificare l'obiettivo di massima armonizzazione (principio di primazia del diritto dell'Unione europea). A ciò si aggiunge che non avrebbe potuto trovare applicazione la disciplina sulle pratiche commerciali scorrette, data la presenza di normative settoriali con riguardo alle quali sarebbe già stato operato un bilanciamento tra protezione dei consumatori e altri interessi specifici considerati dalle leggi speciali (principio della *lex specialis*). E, in terzo luogo, l'AGCM, con riguardo ai fornitori di servizi della società dell'informazione come Meta, non avrebbe potuto imporre obblighi più stringenti rispetto a quelli previsti dalla legge del Paese d'origine del fornitore di servizi. Sotto il profilo della competenza, poi, gli organi legittimati ad intervenire nel caso in esame sarebbero dovuti essere (secondo Meta) la *Data Protection Authority* irlandese (per la condotta *sub a*) ovvero l'informativa resa in fase di prima registrazione alla piattaforma *Instagram*) e la Commissione europea e/o la *Competition and Consumer Protection Commission* irlandese (per le condotte *sub b*), mancata informativa resa in caso di interruzione dei servizi di social network e relati-

[40] Si tratta del provvedimento del 21 maggio 2024, n. PS12566, reperibile sul portale *agcm.it*.

[41] In quanto il professionista, fino al 25 marzo 2024 non ha informato immediatamente, cioè in fase di attivazione e prima registrazione dell'account Instagram via web, dell'attività di raccolta e utilizzo, per finalità commerciali, dei dati dell'utente, così da indurlo ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso (registrazione nella piattaforma IG per usufruire dell'omonimo servizio di *social network*).

[42] In quanto Meta, fino al mese di agosto 2023, contrariamente agli obblighi derivanti dalla diligenza professionale attesa dalla piattaforma, ha omesso: i) con riguardo alla piattaforma *Facebook*, di indicare le modalità (automatizzata o manuale) con cui è stata assunta la decisione di sospendere l'account, ossia di interrompere i propri servizi; ii) con riguardo a entrambi i social network, di fornire indicazioni della possibilità di contestare la decisione di sospendere l'account, oltre che con ricorso interno, anche adendo un organo di risoluzione extragiudiziale delle controversie o ricorrendo a un giudice per contestare la decisione del Professionista e aver previsto un termine relativamente breve (di 30 giorni) per contestare tramite ricorso interno diretto a Meta la decisione del Professionista.

ISSN 2281-3918/2421-2563

vo contraddittorio con l'utente, e *sub c*) mancata assistenza fornita agli utenti che non riescono più ad accedere ai propri *account*).

A ben vedere si tratta di difese superabili come evidenziato dalla stessa AGCM e dai giudici amministrativi già nel precedente caso *Facebook*. In quella vicenda, infatti, l'AGCM riconosceva la propria competenza e coglieva l'occasione sia per delineare i diversi ambiti di operatività del Garante *Privacy* e dell'Autorità *Antitrust*, sia per sostenere la possibile complementarietà della disciplina sulla protezione dei dati personali e di quella concernente le pratiche commerciali scorrette [43]. Ma anche il Tar Lazio respingeva le censure relative alla carenza del potere dell'AGCM, sottolineando il valore patrimoniale dei dati personali [44]. Si deve, tuttavia, al Consiglio di Stato (nella pronuncia n. 2631/2021) la definizione dei rapporti tra la disciplina del GDPR e la tutela consumeristica. Una volta ammessa la patrimonializzazione del dato personale, infatti, la questione non è quella di stabilire se il diritto consumeristico possa o meno sovrapporsi al diritto alla tutela dei dati personali (costituendo tali "diritti" «distinte categorie settoriali» disciplinate da normative speciali e non sovrapponibili tra loro), ma quella di trovare rimedio allo *sfruttamento*, inconsapevolmente per l'utente, dei suoi dati da parte della piattaforma social. E se è vero che la nozione di "trattamento" del dato personale comporterebbe un ambito applicativo amplissimo del GDPR, ciò non significa che lo stesso possa considerarsi "assoluto". «Una siffatta conclusione», si dice, «sarebbe irragionevole, dal momento che ogni scienza giuridica o comportamento umano (…) coinvolge inevitabilmente dati personali» perché porterebbe «ad escludere in radice l'applicabilità di ogni altra disciplina giuridica». Se rimane indiscutibile la "centralità" della disciplina discendente dal GDPR e dai Codici della privacy nazionali «deve comunque ritenersi che allorquando il trattamento investa e coinvolga comportamenti e situazioni disciplinate da altre fonti giuridiche a tutela di altri valori e interessi (altrettanto rilevanti quanto la tutela del dato riferibile alla persona fisica), l'ordinamento – unionale prima e interno poi – non può permettere che alcuna espropriazione applicativa di altre discipline di settore, qual è quella (…) della tutela del consumatore, riduca le tutele alle persone fisiche» [45]. Nella vicenda Meta, l'AGCM, in merito al *principio di specialità*, contesta l'incompatibilità o l'antinomia tra le previsioni in materia di *data protection/privacy* e quelle in materia di protezione del consumatore «perché l'oggetto dell'indagine non afferisce alla correttezza del trattamento dei dati personali da parte della piattaforma» (che avrebbe giustificato l'applicazione delle sole norme sulla *data protection*), «ma alla chiarezza, immediatezza e completezza dell'informazione circa lo sfruttamento di tali dati ai fini commerciali nell'ambito di un "rapporto di consumo"» [46]. Inoltre, con riguardo ai rapporti tra «il complesso sistema di Regolamenti,

[43] Vedi i punti 45-48 del Provvedimento AGCM n. 27432.

[44] A conferma della possibilità di uno sfruttamento economico del dato personale nell'ambito delle "piattaforme social" con conseguente necessità di tutelare il consumatore, i giudici amministrativi richiamano gli *Orientamenti per l'attuazione/applicazione della direttiva 2005/29/CE del 2016* dove la Commissione aveva affermato che "i dati personali, le preferenze dei consumatori e altri contenuti generati dagli utenti hanno un valore economico de facto"; il provvedimento dell'AGCM PS 10601 – *Whatsapp* dell'11 maggio 2017, la decisione della Commissione Europea del 3 ottobre 2014 (pubblicata il successivo 19 novembre 2014) il "network" europeo di autorità nazionali per la cooperazione della tutela dei consumatori di cui al Regolamento 2006/2004/CE.

[45] Ad avviso del Collegio, quindi, non serve creare "compartimenti stagni di tutela" ma occorre piuttosto garantire "tutele multilivello" che possano amplificare il livello di garanzia dei diritti delle persone fisiche, anche quando un diritto personalissimo sia "sfruttato" a fini commerciali, indipendentemente dalla volontà e, soprattutto, senza la consapevolezza (da parte) dell'interessato consumatore.

[46] Di recente cfr. anche Cons. Stato, sez. VI, 7 gennaio 2025, n. 80 (caso Google Ireland Ltd.), in Banca dati *De Jure*, dove si afferma (vedi punto 2.1.1): «la giurisprudenza europea e la giurisprudenza nazionale hanno ritenuto che al criterio della

ISSN 2281-3918/2421-2563

Direttive, norme di *soft law* e norme di autoregolamentazione che disciplinerebbero compiutamente e con un approccio multilivello i c.d. servizi intermediari» e la disciplina consumeristica sulle pratiche commerciali scorrette, non solo ribadisce il carattere *orizzontale* e *prevalente* del Codice del consumo la cui nozione di pratica commerciale è così ampia da estendersi a tutte le attività poste in essere dai professionisti (anche nei confronti degli utenti di servizi digitali) prima, durante e dopo l'operazione commerciale [47], ma si ritiene anche che non vi sia contrasto tra il Regolamento (UE) 2022/2065 (*Digital Services Act – DSA*) e le disposizioni a tutela del consumatore in quanto è lo stesso DSA a fare espressamente salvo il diritto europeo in materia di tutela dei consumatori [48].

Quanto, poi, alla presunta violazione, da parte dell'AGCM, del principio del Paese di origine (sulla base delle affermazioni contenute nella pronuncia della Corte di giustizia *Meta Platforms Ireland and Others vs KommAustria* [49]) «che impedirebbe all'Autorità di imporre al Professionista obblighi "regolamentari" diversi da quelli previsti dall'ordinamento ove il Professionista si è stabilito», l'AGCM si difende affermando la compatibilità della disciplina consumeristica con tale principio e con la Direttiva *E-Commerce* (da cui lo stesso viene desunto) in quanto, nel caso di specie, si rientrava nelle ipotesi di deroga al principio di stabilimento ivi "codificate" [50]. Nel merito delle violazioni, poi, trascurando la pratica scorretta consistente nell'aver ingannato i consumatori per non averli informati sull'utilizzo, per finalità commerciali dei dati raccolti, qualche osservazione può farsi con riguardo all'ingannevolezza della condotta di Meta per aver omesso di indicare ai suoi utenti le modalità per contestare i provvedimenti di sospensione del loro *account*, oltre che con ricorso interno, anche adendo un organo di risoluzione stragiudiziale delle controversie o ricorrendo ad un giudice per contestare la decisione del Professionista. Correttamente l'AGCM considera questa pratica contraria alla diligenza professionale che, ai sensi dell'art. 20 cod. cons., è uno dei parametri per qualificare la pratica commerciale come scorretta. Il comportamento di Meta infatti, per un verso, impedisce agli utenti di esercitare il diritto di difesa [51] e, per altro verso, preclude loro di svolgere le attività sociali o professionali considerate essenziali nella società contemporanea. Secondo l'AGCM «Il Professionista diligente avrebbe …

---

specialità, che vedrebbe prevalere la competenza dell'Autorità settoriale, debba preferirsi il criterio dell'incompatibilità, che vede possibile l'intervento dell'Autorità di settore solo qualora la condotta contestata abbia "ambiti specifici", nel senso che non rientri nel potere di intervento dell'Antitrust». Di conseguenza «laddove la condotta contestata è tale da rientrare in astratto nel potere di intervento di ambedue le Autorità, la competenza è dell'Antitrust, non dell'Autorità di settore». Nello stesso senso cfr. le pronunce della sesta sezione del Cons. Stato 9 luglio 2024, n. 6077; 5 giugno 2024, n. 5030 e 5 aprile 2024, n. 3175.

[47] Peraltro, a supporto, della propria tesi l'AGCM richiama sia il precedente della Corte di giustizia UE, cause riunite C-54/17 e C-55/17 del 13 settembre 2018, cit. (dove il "contrasto" tra le disposizioni di detta direttiva e altre norme comunitarie sussiste solo laddove queste ultime disciplinino aspetti specifici delle pratiche commerciali sleali imponendo ai professionisti, senza alcun margine di manovra, obblighi incompatibili con quelli stabiliti dalla direttiva 2005/29/CE), sia l'art. 27, comma 1-*bis*, cod. cons., che assegna in via esclusiva all'AGCM l'*enforcement* rispetto a tutte le condotte che danno luogo a una pratica commerciale scorretta, comprese quelle che integrano anche la violazione di altre norme di settore.

[48] Vedi art. 2 e considerando n. 10 del DSA.

[49] Si tratta di CGUE 9 novembre 2023, C-376/22 consultabile su *www.eius.it*.

[50] Per l'art. 3, par. 4, della suddetta direttiva le eccezioni al principio di stabilimento sono ammissibili se i provvedimenti presi sono necessari alla tutela dei consumatori; concernono servizi della società dell'informazione e sono proporzionati a tali obiettivi. Queste condizioni ricorrevano tutte nel caso di specie dove l'AGCM aveva preso un provvedimento "necessario" e "proporzionato" alla salvaguardia dei consumatori e concernente servizi della società dell'informazione come i servizi Facebook e Instagram.

[51] La mancata indicazione al consumatore della possibilità di ricorrere al giudice ordinario o di sfruttare meccanismi stragiudiziali di risoluzione delle controversie (ADR) potrebbero indurlo a ritenere di disporre del solo reclamo interno, peraltro da esperire nel breve termine di 30 giorni e, quindi, di una tutela davvero risicata.

ISSN 2281-3918/2421-2563

senz'altro dovuto fornire ai soggetti privati del servizio la più ampia informativa, anche circa le modalità di contestazione ed eventuale risoluzione delle problematiche riscontrate, al fine di "reintegrare" nel *social network* l'utente attinto dalla misura sospensiva».

4 – L'utilizzo di dati personali a fini commerciali può dar vita a comportamenti abusivi non soltanto nei confronti dei consumatori ma anche delle imprese concorrenti. Qualche anno fa, infatti, l'autorità tedesca per la concorrenza, la *Bundeskartellamt* (*BKartA*) nella decisione del 6 febbraio 2019, B6-22/16, condannava Facebook a modificare le proprie condizioni di servizio laddove condizionava la fornitura dello stesso alla circostanza che gli utenti fornissero dati ulteriori rispetto a quelli necessari per l'accesso al social network, cioè i dati prodotti dall'utilizzo di *Wathsapp* e *Instagram,* nonché quelli raccolti su siti di terze parti. Tale comportamento per l'Autorità amministrativa tedesca poteva essere ricondotto ad un abuso di posizione dominante mediante il quale si frustrava il diritto all'autodeterminazione degli utenti che si vedevano imposte condizioni generali di contratto inique in quanto violavano diritti costituzionali come quelli protetti dal GDPR [52]. Il *trait d'union* tra concorrenza e protezione dei dati personali era dato dal fatto che i dati usati senza il valido consenso degli utenti veniva considerato come fattore che abbassava la qualità della concorrenza. Di parere diverso era, invece, la Corte d'appello tedesca per la quale il *BKartA* non aveva svolto le indagini necessarie sulla violazione da parte di *Facebook* delle regole sulla concorrenza [53]. Tuttavia il 23 giugno 2020 la Corte federale di giustizia tedesca, nella decisione KVR69/19, dà ragione al *BKartA* e riconosce in capo a *Facebook* la posizione dominante nel mercato tedesco dei social network e il conseguente abuso di posizione dominante. È indubbio, infatti, che la capacità di profilazione raggiunta da Facebook le garantiva un significativo potere di mercato, irraggiungibile da parte dei *competitors*, impossibilitati a combinare altrettanti dati, ma il problema non stava nella posizione dominante quanto nell'abuso di essa dovuto all'impiego di condizioni contrattuali che vincolavano, senza margine di scelta, gli utenti a subire la combinazione delle varie fonti per la costruzione dei loro profili [54].

---

[52] Per il BKarta il comportamento concreto di Facebook e la quantità dei dati elaborati provavano l'abuso da sfruttamento di cui all'art. 102 TFUE.

[53] Si contesta anche la "perdita di controllo dei dati" da parte dell'interessato e la violazione del suo diritto all'autodeterminazione informativa. Il fatto che per accedere al servizio social si richieda il consenso all'uso di dati aggiuntivi non significa, per i giudici di appello, una perdita di controllo dei dati (con pregiudizio alla sfera giuridica dell'interessato), ma «rende soltanto necessario *bilanciare i vantaggi* derivanti dall'uso di un social network finanziato dalla pubblicità (e quindi gratuito) *con le conseguenze* associate all'uso dei dati aggiuntivi da parte di Facebook. L'utente può compiere questa valutazione senza essere influenzato e in completa autonomia, in base alle sue preferenze e ai suoi valori personali». Così M. MIDIRI, *Privacy e antitrust*, cit., 225, che riporta il passo dell'OLG di Düsseldorf.

[54] La vicenda tedesca ha consentito alla dottrina di compiere delle riflessioni più generali con riferimento sia alla patrimonializzazione dei dati che all'utilizzo del GDPR per arginare fenomeni di abuso di posizione dominante. Al riguardo G. D'ACQUISTO-F. PIZZETTI, *Regolamentazione dell'economia dei dati e protezione dei dati personali*, in *Analisi giur. econ.*, 1/2019, 97 evidenziano come la pronuncia del BKartA testimoni l'idoneità del trattamento dati personali a creare valore economico e l'idoneità della profilazione derivante dalla combinazione di dati tra diverse sorgenti di creare squilibri nelle dinamiche competitive del mercato. Per gli A. è rilevante la circostanza che un'Autority nazionale antitrust intervenga per riequilibrare questa situazione di *exploitative abuse* con strumenti propri di settori diversi come il GDPR, anche in considerazione del fatto che alla base della lesione della concorrenza vi era la mancanza di un consenso libero e consapevole da parte degli interessati al trattamento dei dati richiesti, difetto che rendeva illecito il trattamento dei dati personali anche ai sensi del GDPR. Il BKartA, intervenendo con strumenti di data protection, finiva per ottenere la riallocazione di un valore economico, illegittimamente fatto proprio da Facebook, presso competitors rendendo loro accessibili quote di mercato da cui erano precedentemente esclusi.

ISSN 2281-3918/2421-2563

La decisione del BKartA – con cui si affermava un approccio *integrato* tra disciplina a tutela dei dati personali e disciplina antitrust – è stata criticata perché ritenuta in contrasto con l'orientamento dominante e, in particolare, con quello seguito dalla Commissione europea in materia di concentrazioni. Infatti, in una serie di casi [55] sottoposti alla sua valutazione, la Commissione europea, pur progressivamente riconoscendo il ruolo della privacy come parametro rilevante nella concorrenza fra piattaforme online, non ha bloccato alcuna operazione approvando, quasi sempre senza condizioni, le concentrazioni che sollevavano criticità dal punto di vista della privacy, a conferma dell'approccio separatista per il quale queste due aree del diritto devono restare distinte in quanto assolvono a funzioni e tutelano obiettivi diversi. Analogamente può dirsi con riferimento alle scelte della nostra AGCM che, ad esempio, per comportamenti discriminatori attuati da *Google* nel mercato del *digital adversiting*, ha utilizzato un tipo di contestazione diversa da quella adottata dal BKartA.

La nostra Autorità, infatti, nel valutare il presunto abuso di posizione dominante di *Google* non si interroga sulla conformità alla normativa sulla privacy della politica adottata dalla società per raccogliere il consenso degli utenti al trattamento dei loro dati, e, quindi, sulla liceità dei mezzi impiegati a tal fine, ma considera i meccanismi attraverso i quali Google sfruttava quei dati a proprio vantaggio. A parere dell'AGCM "la condotta posta in essere da Google le permette di mantenere una capacità di offerta di servizi di intermediazione nei suddetti mercati della pubblicità a condizioni e con modalità non replicabili dai concorrenti, tali da rappresentare un vantaggio competitivo ingiustificato. Facendo leva sui dati ottenuti attraverso tali strumenti, non accessibili a terzi, Google consente alla propria *Google Marketing Platform* (ovvero la sua DSP) e al proprio *Google Ad Manager* (SSP) di avere prestazioni in termini di capacità di targhettizzazione e di identificazione degli utenti che visualizzano inserzioni pubblicitarie che non sono altrimenti raggiungibili da parte di altri operatori del mercato» [56]. Anche la dottrina [57] non ha mancato di mettere in evidenza i rischi di desumere dalla lesione della disciplina sulla *data protection*

---

[55] Si tratta, in primo luogo del caso *Google/DoubleClik* dell'11 marzo 2008, M.4731. In questa vicenda, ferma restando la posizione dominante nel mercato di riferimento, la Commissione ha ritenuto che la società risultante dalla fusione di Google e DoubleClik (e dei loro dataset) non avrebbe ottenuto un potere tale da escludere i suoi concorrenti e da impedire la libera concorrenza sul mercato. Nello specifico non vi erano indicazioni che l'impresa risultante sarebbe stata in grado di imporre ai suoi clienti variazioni delle condizioni contrattuali idonee a consentire successivamente l'utilizzo incrociato dei loro dati. Nelle sue Conclusioni la Commissione evidenzia la compatibilità dell'operazione di fusione societaria con la disciplina in materia di concentrazioni ma non esclude possibili rischi per la tutela dei dati personali, dimostrando di tenere distinti gli ambiti applicativi delle due discipline. Ciò conferma che l'eventuale riduzione della tutela della privacy, derivante dalla suddetta fusione societaria e dei *dataset*, non rientra nel campo di applicazione del diritto antitrust ma è materia di *data protection*. Questo orientamento che sembrava incrinarsi nella vicenda, decisa dalla Commissione il 6 dicembre 2016, *Microsoft/Linkedin* (M.8124 – *Microsoft/Linkedin*) è stato confermato qualche anno più tardi nell'operazione di concentrazione tra *Google* e *Fitbit* (decisione del 17 dicembre 2020, M.9660) e nella più recente decisione del 10 febbraio 2023, M.10815 – *Deutsche Telekom, Orange/Telefonnica/Vodafone/Jv*, dove si è ritenuta conforme alla concorrenza la creazione di una *joint venture* di queste importanti società di telefonia per mettere in comune i dati relativi a tutti gli utenti, sempre ai fini di profilazione e pubblicità commerciale. Tutte le decisioni sono consultabili sul sito *https://competition-cases.ec.europa.eu*.

[56] Si tratta di AGCM, Provvedimento n. 28938 del 20 ottobre 2020, consultabile sul sito *www.agcm.it*. Più di recente l'AGCM, nel Provvedimento n. 30215 del 5 luglio 2022, caso *Google* e *Alphabet*, ha avviato un'altra istruttoria per presunta violazione della concorrenza *ex* art. 102 TFUE e art. 3, legge n. 287/1990, in quanto il gruppo Google avrebbe ostacolato l'interoperabilità nella condivisione dei dati presenti nella propria piattaforma con altre piattaforme, così comprimendo il diritto alla portabilità dei dati degli utenti interessati (art. 20 GDPR) e determinando una restrizione della concorrenza. Tuttavia, a seguito della presentazione da parte di Google di un pacchetto di impegni volti ad evitare proprie condotte anticoncorrenziali, l'AGCM ha chiuso la procedura ritenendo tali impegni compatibili con il diritto antitrust.

[57] Tra gli altri cfr. G. COLANGELO-M. MAGGIOLINO, *Data Protection in Attention Markets: Protecting Privacy Trough Competition?*, in *Journal of European Competition Law & Practice*, 2017, 9 ss.

ISSN 2281-3918/2421-2563

l'automatica violazione della disciplina antitrust, in considerazione del fatto che si tratta di apparati regolatori volti a perseguire obiettivi diversi e che presentano peculiarità tali da potersi anche porre in contrasto tra loro. Ritenerli necessariamente convergenti, allora, potrebbe generare non poca confusione [58].

L'idea di basare la connessione tra privacy e antitrust considerando la *policy privacy* quale componente della qualità di un prodotto o servizio per cui la riduzione di tutela della privacy coincide automaticamente con una degradazione della qualità dei beni o servizi offerti con danni sia al benessere del consumatore che alla concorrenza, non coglie nel segno. Si potrebbe dire che la massiva raccolta ed elaborazione di dati da parte delle piattaforme online sia fatta proprio per aumentare la qualità dei servizi offerti e non per degradarla [59]. E, soprattutto, non sono rari i casi in cui le piattaforme online modificano la loro *policy privacy* rendendola più rigorosa non al fine di tutelare i consumatori e migliorare la qualità dei servizi offerti ma per aumentare le barriere all'ingresso nel mercato dei pochi concorrenti e, quindi, come strategia anticoncorrenziale [60]. In tal caso è evidente la "tensione", la "contrapposizione" (piuttosto che la simmetria) tra diritto alla protezione dei dati e la concorrenza. Esemplare, in quest'ottica è il caso *Apple* (A561) destinatario di un'istruttoria dell'AGCM volta ad accertare l'esistenza di un presunto abuso di posizione dominante di *Apple* nel mercato delle piattaforme per la distribuzione online di *app* per utenti del sistema operativo iOS [61]. Infatti, la nuova *policy privacy* di Apple, realizzata attraverso l'*App Tracking Transparency* (ATT) e rivolta ai soli sviluppatori di *app* terzi, aveva diminuito in modo drastico e discriminatorio la loro capacità di raccogliere dati e di profilare gli utenti, riducendo così il valore degli spazi pubblicitari da questi venduti agli inserzionisti. *Apple* aveva ostacolato a proprio vantaggio la capacità dei concorrenti di vendere spazi pubblicitari, aveva favorito le proprie vendite (dirette e indirette) e aveva ridotto il potere contrattuale degli inserzionisti concentrando l'offerta degli spazi pubblicitari nelle proprie mani. La condotta di *Apple* era idonea, quindi, a creare barriere all'ingresso nel mercato della distribuzione delle *app* agli sviluppatori concorrenti e a favorire le sue *app* e le sue vendite, in violazione dell'art. 102 TFUE. Sebbene il caso *Apple* abbia messo in evidenza i rischi connessi all'approccio integrato privacy-antitrust, l'idea che le norme in materia di protezione dei dati personali possano considerarsi parametro per valutare la correttezza della condotta delle imprese in base alla disciplina antitrust è stata fatta propria, da qualche anno, anche dalla Corte di giustizia UE nella causa *Meta Platforms e a.* (*Condizioni generali d'uso di un social network*) del 4 luglio 2023 [62]. La vicenda ha rappresentato l'occasione per far luce anche sui rapporti

---

[58] Perplessità in tal senso sono espresse da G. COLANGELO, *The Privacy – Antitrust Curse: Insights fron GDPR Application in EU Competition*, in *International centre for Law and Economics*, ICLE White Paper 2023, 5.

[59] E quindi, per dirla con G. COLANGELO, *Big. Data, Piattaforme digitali e antitrust*, in *MCR*, 2016, 12, 454, «mancherebbe il legame tra presunta degradazione della qualità e benessere dei consumatori: mentre, infatti, alcuni vedranno in interventi più invasivi per raccogliere e utilizzare dati una diminuzione della qualità, altri riterranno che annunci pubblicitari e servizi maggiormente personalizzati rappresentino un miglioramento qualitativo». Peraltro, La stessa degradazione della qualità è concetto "sfuggente" e, comunque, sarebbe difficile spiegare come l'autorità possa essere in grado di misurare la migliore qualità assicurabile ai consumatori, data la soggettività di tale parametro.

[60] Parla di privacy come "scudo" per legittimare condotte anticoncorrenziali G. COLANGELO, *The Privacy – Antitrust Curse: Insights fron GDPR Application in EU Competition*, cit., 23.

[61] Si tratta di AGCM, Istruttoria A561 – *Apple/ATT*; Provvedimento del 5 maggio 2023, n. 30620, in *www.agcm.it*.

[62] Si tratta della causa C-252/21 in ECLI:EU:C:2023:537, con commento di E. DE FALCO in *www.deiustitia.it* e di A. PALMIERI, *Prevaricazioni ascritte al gestore di un social network tra antitrust e* data protection (Nota a CGUE, sez. grande, 4/7/2023 n. 252), in *ForoNews* 5 luglio 2023, banca dati *Foroplus*. Ma vedi anche l'interessante contributo critico di A. D'AVOLA, *«*More than meets the eye?*». Riflessioni critiche e prospettive d'indagine (sull'incrocio tra privacy e antitrust) a valle del caso* Meta, in *Foro it*., 12/2023, 579 ss.

ISSN 2281-3918/2421-2563

tra le diverse *Autorithy* quando, tramite la violazione dell'RGDP, viene contemporaneamente lesa la concorrenza. Nel caso in questione, infatti, la registrazione sulla piattaforma social Facebook (gestita in Europa da *Meta Platforms Ireland*) implicava, per gli utenti, l'accettazione delle condizioni generali stabilite da questa società, compresi la politica sulla privacy e l'uso dei *cookie*. Tali condizioni prevedevano che *Meta Platforms Ireland* potesse raccogliere i dati degli utenti sia all'interno che all'esterno del *social network* (c.d. dati *off* Facebook) affinché venissero utilizzati per fornire loro una pubblicità personalizzata. L'Autorità garante per la concorrenza tedesca (*BKartA*) ha vietato la pratica di Facebook di condizionare l'uso del social da parte degli utenti tedeschi al trattamento dei loro dati *off* Facebook senza il loro esplicito consenso in quanto si trattava di un trattamento che violava l'RGDP e integrava un abuso di posizione dominante di *Meta Platforms Ireland* sul mercato tedesco dei *social network online*. Il Tribunale superiore del Land, Düsseldorf, adito da Meta per contestare la decisione del Garante tedesco, ha posto alla Corte di giustizia la questione se le autorità nazionali responsabili della concorrenza e del mercato potessero o meno verificare la conformità di un trattamento dei dati ai requisiti stabiliti dal RGDP ed ha chiesto chiarimenti su alcune disposizioni del Regolamento concernenti il trattamento dei dati da parte di un operatore di un *social network online* (in particolare gli artt. 6 e 9, parr. 1 e 2).

La Corte di giustizia, esaminate le sette questioni pregiudiziali proposte, ha ritenuto che gli artt. 51 ss. RGDP e gli artt. 4, par. 3, TFUE debbano essere interpretati nel senso che «fermo restando il rispetto del suo obbligo di leale cooperazione con le autorità di controllo, un'autorità garante della concorrenza di uno Stato membro può constatare, nell'ambito dell'esame di un abuso di posizione dominante da parte di un'impresa, …, che le condizioni generali d'uso di tale impresa relative al trattamento dei dati personali e la loro applicazione non sono conformi a detto regolamento, qualora tale constatazione sia necessaria per accertare l'esistenza di un tale abuso».

Tuttavia, accertata una violazione dell'RGDP, l'autorità garante della concorrenza non può (né deve) assumere il ruolo che spetta al Garante *privacy*, ma può soltanto verificare se tale violazione costituisca elemento di possibile alterazione della dinamica concorrenziale e quindi, ad esempio, di un abuso di posizione dominante, per porvi fine [63]. E, comunque, il principio di leale cooperazione tra le autorità di controllo implica che laddove il garante nazionale della concorrenza ritenga di dover valutare se il comportamento di un'azienda sia conforme alle disposizioni del GDPR, deve prima verificare se tale comportamento o uno simile sia già stato oggetto di una decisione da parte del competente Garante *privacy* o della Corte di giustizia e non può discostarsi dalla loro decisione («pur restando libera di trarne le proprie conclusioni sotto il profilo dell'applicazione del diritto della concorrenza») [64]. Il profilo di maggiore impatto della decisione è dato, però, dalla considerazione, da parte dei giudici europei, della violazione della disciplina in materia di dati personali quale presupposto costitutivo dell'illecito anticoncorrenziale, per l'importanza economica che hanno sempre più assunto l'accesso ai dati personali ed il loro sfruttamento quali parametri significativi della concorrenza tra imprese dell'economia digitale. Difatti, le imprese che avranno un maggiore accesso ai dati degli utenti e tratteranno una quantità maggiore di dati saranno favorite sul mercato rispetto alle altre. Se, poi, le stesse svolgeranno

[63] La distinzione delle competenze tra autorità nazionali di controllo (circa il rispetto del Regolamento europeo sulla *privacy*) e autorità nazionali antitrust è messa bene in luce nei punti 44-46 della sentenza in esame.

[64] Ciò serve ad evitare che l'Autorità Antitrust invada illegittimamente le competenze dell'Autorità garante della protezione dei dati personali.

ISSN 2281-3918/2421-2563

tale attività in violazione della normativa del GDPR matureranno dei vantaggi competitivi illeciti con un impatto significativo, ed al contempo negativo, sulla concorrenza leale tra imprese.

Si comprende, allora, l'affermazione della Corte di giustizia per cui «escludere le norme in materia di protezione dei dati personali dal contesto giuridico che le autorità garanti della concorrenza devono prendere in considerazione in sede di esame di un abuso di posizione dominante ignorerebbe la realtà di tale evoluzione economica e potrebbe pregiudicare l'effettività del diritto della concorrenza all'interno dell'Unione». Se questo è vero, però, occorre rifuggire da qualunque automatismo per il quale basterebbe la sola violazione delle norme del GDPR a configurare anche l'illecito concorrenziale. Non foss'altro perché il diritto della concorrenza risponde a logiche diverse da quelle che animano altri settori del diritto (inclusa la privacy), con la conseguenza che una determinata azione può essere idonea ad alterare le dinamiche concorrenziali sebbene sia *privacy compliant* (anzi, come abbiamo detto, a volte il più elevato rispetto della privacy può nascondere delle strategie anticoncorrenziali, *Apple ATT docet!*) e, al contempo, per aversi illecito concorrenziale il mancato rispetto della privacy non è sufficiente se non si accompagna a tutte le altre condizioni necessarie per qualificare una condotta come anticoncorrenziale [65] (posizione di dominanza dell'impresa sul mercato, esistenza di un mercato rilevante dove essa opera, abusività della condotta per acquisire vantaggi competitivi, danno economico alle concorrenti e nesso di causalità condotta-danno). A ragionare diversamente si offuscherebbe una peculiarità del diritto antitrust: la sua *neutralità* rispetto alla liceità formale della condotta imprenditoriale, in quanto ciò che conta è soltanto verificare quali siano i suoi effetti sul mercato. Altre questioni riguardano, poi, le categorie di dati trattati e la libertà del consenso prestato dall'interessato. Quanto ai dati si è posto, innanzitutto, il problema dei dati raccolti dal gestore del *social network online* tramite interfacce integrate, *cookie* ecc., dati che gli utenti hanno concesso per la consultazione di siti web e applicazioni e che vengono ricollegati al loro *account* nel *social network online* ma che possono rivelare informazioni delicate, rientranti nelle categorie di cui all'art. 9, par. 1, RGDP (quindi informazioni sull'origine razziale o etnica, sulle opinioni politiche e religiose, sulla vita e l'orientamento sessuale degli interessati). Proprio per queste caratteristiche la Corte di giustizia considera che, qui, il trattamento abbia ad oggetto categorie particolari di dati e, quindi, sia in linea di principio vietato. Con riguardo, poi, alla possibilità di consentire eccezionalmente il trattamento di tali dati sensibili quando gli stessi siano «resi manifestamente pubblici dall'interessato», la Corte chiarisce che le eccezioni al divieto di trattamento di cui al par. 2 dell'art. 9 RGDP debbano essere interpretate restrittivamente, occorrendo verificare in concreto se l'interessato avesse inteso, «in modo esplicito» e «con un atto positivo chiaro», rendere accessibili al pubblico i dati medesimi (art. 9, par. 2, lett. *e*). Questa volontà inequivoca non emerge dalla mera consultazione dei siti internet e delle applicazioni in quanto – si dice – in tali casi l'utente «può attendersi che il gestore del sito o dell'applicazione abbia accesso a tali dati e che li condivida», se del caso e fermo restando il suo consenso esplicito con alcuni terzi ma non con il pubblico [66]. E, persino nelle ipotesi in cui gli utenti inseriscano volontariamente i loro dati

[65] Lo specifica bene A. D'AVOLA, *op. cit.*, 592 laddove afferma che il nesso causale (tutto normativo) tra violazione del GDPR e danno alla concorrenza, creato dalla Corte di giustizia UE, finisce per «destrutturare» la stessa fattispecie anticoncorrenziale perché non tiene in considerazione i presupposti che necessariamente determinano l'illecito *ex* art. 102 TFUE, e ciò finisce per delineare una sorta di responsabilità antitrust oggettiva «ogniqualvolta si riscontri la violazione di norme imperative, passate da elemento presuntivo e indiziario (…) a vera e propria pietra angolare del procedimento».

[66] Al punto 79 della pronuncia in commento si precisa che «dalla mera consultazione dei siti internet o delle applicazioni da parte di un utente non si può dedurre che detti dati personali siano stati manifestamente resi pubblici dall'utente». Questo è

ISSN 2281-3918/2421-2563

in siti internet o applicazioni, attivando pulsanti di condivisione integrati (del tipo «Mi piace» o «Condividi»), si può dire che ci sia la loro volontà univoca di rendere manifestamente pubblici i dati che li riguardano solo se abbiano espresso consapevolmente e in anticipo la scelta di rendere i propri dati accessibili pubblicamente ad un numero illimitato di persone [67]. Chiarita l'interpretazione da dare ai paragrafi 1 e 2 dell'art. 9 RGDP, la Corte analizza le questioni sollevate dal giudice del rinvio con riferimento all'interpretazione dell'art. 6 dell'RGDP che, com'è noto, introduce delle giustificazioni per consentire il trattamento di dati personali, altrimenti vietato anche in considerazione della mancanza di un consenso espresso dell'interessato. Si tratta delle ipotesi in cui il trattamento può essere considerato necessario per l'esecuzione di un contratto del quale gli interessati sono parti (lett. *b*), o per il perseguimento del "legittimo interesse" del titolare del trattamento o di terzi (lett. *f*), o per adempiere un obbligo legale al quale è soggetto il titolare del trattamento o per salvaguardare gli interessi vitali dell'interessato o per realizzare fini di pubblico interesse.

Tuttavia, nel caso sottoposto al suo giudizio, la Corte di giustizia esclude sia che il trattamento dei dati effettuato da *Meta Platforms Ireland* fosse necessario all'esecuzione del contratto con i suoi utenti, sia che lo stesso fosse essenziale al perseguimento del legittimo interesse del titolare del trattamento o di terzi. L'ultimo profilo, per noi importante, è costituito dall'interpretazione che la Corte di giustizia offre dell'art. 6, par. 1, comma 1, lett. *a* e dell'art. 9, par. 2, lett. *a*, RGDP. Si discute se il consenso prestato dall'interessato con riferimento al trattamento di categorie particolari di dati (*ex* art. 9, par. 1, lett. *a*) soddisfi le condizioni di validità previste dall'art. 4, punto 11, dell'RGDP e, in particolare, quella secondo cui tale consenso deve essere prestato liberamente, qualora il titolare del trattamento occupi una posizione dominante nel mercato dei *social network online*.

Secondo la Corte, la circostanza che il titolare del trattamento occupi una posizione dominante nel mercato dei social network «non osta, di per sé, a che gli utenti di tale *social network* possano validamente acconsentire, ai sensi dell'art. 4, punto 11, RGDP, al trattamento dei loro dati personali effettuato da tale operatore». Tuttavia, la posizione dominante del titolare del trattamento impatta sulla validità e sulla libertà del consenso [68] prestato dall'utente del *social network*, ed accentua la condizione di squilibrio esistente tra l'interessato ed il titolare del trattamento, in quanto favorisce l'imposizione di condizioni che non sono strettamente necessarie all'esecuzione del contratto. Sarà il titolare del trattamento a dover dimostrare che non è così e, quindi, ad esempio, che il trattamento dei dati non era necessario all'esecuzione del contratto [69], che gli utenti disponevano della libertà di rifiutare, nell'ambito della procedura contrattuale, di prestare il loro consenso senza per questo essere costretti a rinunciare al servizio offerto dall'operatore del *social network online*, o comunque che era data agli utenti medesimi la possibilità di prestare un consenso separato per i dati *off* Facebook rispetto a quello necessario per il trattamento dei dati relativi alla fruizione del servizio social.

Che la violazione della normativa sulla protezione dei dati personali integrante una pratica commerciale sleale possa essere fatta valere oltre che dall'Autorità antitrust anche da una concorrente dell'impresa responsabile della condotta scorretta è, poi, l'ulteriore principio affermato dalla Grande

---

un aspetto che la Corte di giustizia ha confermato anche nella recente sentenza della Corte di giustizia, 4 ottobre 2024, n. 446, causa C-446/21, *Ma. Sc. vs. Meta Platforms Ireland Ltd*., consultabile in Banca dati *DeJure*.

[67] Vedi punto 83 della sentenza.

[68] Sulla libertà del consenso assumono rilievo i considerando 42 e 43 del RGDP.

[69] Condizione che l'art. 7, par. 4 RGDP pone come necessaria per assicurare la libertà del consenso.

ISSN 2281-3918/2421-2563

Sezione della Corte di giustizia UE nella causa C-21/23 del 4 ottobre 2024 [70]. La vicenda riguardava una controversia insorta tra due gestori di farmacie in Germania, uno dei quali commercializzava sulla piattaforma online *Amazon – Marketplace* medicinali la cui vendita era riservata alle farmacie, senza che fosse garantito ai clienti di dare il loro consenso preventivo al trattamento dei dati relativi alla salute. Si lamentava una vendita sleale dei medicinali, irrispettosa dei requisiti di legge relativi all'ottenimento del consenso da parte del cliente, per come richiesto dalla normativa in materia di protezione dei dati personali. Il ricorso ha trovato accoglimento nel primo grado di giudizio e la soluzione è stata poi confermata anche in appello dove si è ritenuto che la commercializzazione su Amazon di medicinali la cui vendita era riservata alle farmacie integrasse una pratica sleale, illecita per la legge tedesca contro la concorrenza sleale [71]. La condotta dell'impresa venditrice, infatti, avrebbe violato l'RGDP perché, in contrasto con l'art. 9, parr. 1 e 2, avrebbe trattato dati relativi alla salute degli acquirenti dei medicinali in assenza del loro consenso espresso. Ma soprattutto, per i giudici europei le norme dell'RGDP indicano anche il comportamento che le imprese devono tenere sul mercato per non violare la legge nazionale sulla concorrenza con la conseguenza che, in caso contrario, il concorrente leso, ai sensi dell'art. 8, par. 3, punto 1, dell'UWG, avrebbe diritto di dedurre la violazione mediante un'azione inibitoria dinanzi ai giudici civili.

Nel silenzio del GDPR che (a differenza dell'art. 8, par. 1 dell'abrogata dir. 95/46) non menziona, né esclude, la possibilità per i concorrenti dell'impresa sleale di poter ricorrere al giudice civile per far cessare le violazioni delle disposizioni sulla privacy commesse dalla stessa impresa sulla base del divieto di pratiche commerciali sleali, tale possibilità è stata argomentata dalla Corte di giustizia sulla base di un'analogia con quanto già sostenuto, in altra pronuncia [72], a favore delle associazioni consumeristiche, cui era stato riconosciuto il potere di agire in giudizio (anche in assenza di mandato e indipendentemente dalla violazione di specifici diritti degli interessati) contro il presunto autore di un atto pregiudizievole per la protezione dei dati personali, facendo valere la violazione della disciplina a tute-

---

[70] La pronuncia è consultabile su ECLI:EU:C: 2024:846.

[71] Si tratta dell'art. 3, par. 1, dell'UWG (*Gesetz gegen den unlauteren Wettbewerb* del 3 luglio 2004), intitolato «Divieto di comportamenti commerciali sleali», per il quale «Le pratiche commerciali sleali sono illecite». L'art. 3a dell'UWG, poi, prevede che «Commette un atto sleale colui il quale violi una disposizione di legge che sia altresì destinata a disciplinare il comportamento sul mercato nell'interesse dei soggetti partecipanti al mercato stesso, nel caso in cui la violazione sia idonea a pregiudicare in maniera sensibile gli interessi dei consumatori, di altri soggetti partecipanti al mercato o dei concorrenti»

[72] Si tratta di CGUE 28 aprile 2022, causa C-319/20, *Meta Plartforms Ireland Limited vs Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e. V.*, in ECLI:EU:C:2022:322 (su cui vedi il commento di M. FEDERICO, *Rappresentanza degli interessati, diritti individuali e Group Data Protection*, in *Persona e mercato*, 2022,4, 674 ss. e di A. PALMIERI, *L'ambito della tutela collettiva contro gli atti pregiudizievoli per la protezione dei dati personali (Nota a CGUE 28/4/2022)*, in *ForoNew*s 4 maggio 2022, banca dati Foroplus) dove la Corte di giustizia precisa che nella controversia di cui al procedimento principale non viene in questione la legittimazione ad agire di un concorrente, bensì quella delle associazioni e di altri organismi contemplati dall'art. 80, par. 2, RGDP. Pertanto, la questione sollevata dal giudice di rinvio si traduce nel quesito se l'art. 80, par. 2, RGDP debba essere interpretato nel senso che esso osta ad una normativa nazionale che consente ad un'associazione di tutela degli interessi dei consumatori di agire in giudizio, in assenza di specifico mandato e indipendentemente dalla violazione di specifici diritti di un interessato, contro il presunto autore di un atto pregiudizievole per la protezione dei dati personali, facendo valere la violazione del divieto di pratiche commerciali sleali, la violazione di una legge in materia di tutela dei consumatori o la violazione del divieto di utilizzazione di condizioni generali di contratto nulle (vedi punti 50 e 51 della sentenza). La Corte da risposta negativa al quesito ammettendo l'azione in giudizio anche delle associazioni consumeristiche contro il presunto autore di un atto pregiudizievole per la protezione dei dati personali, quando lo stesso pregiudichi anche le norme poste a tutele dei consumatori o contro le pratiche commerciali scorrette «qualora il trattamento di dati in questione sia idoneo a pregiudicare i diritti riconosciuti da tale regolamento a persone fisiche identificate o identificabili».

ISSN 2281-3918/2421-2563

la dei consumatori. La stessa Corte si era posta il problema del possibile contrasto con l'obiettivo di uniformazione perseguito dal Regolamento privacy dato dalla possibilità, per i concorrenti, di agire ai sensi del diritto antitrust, facendo applicazione delle norme dell'RGDP oltre i limiti in esso previsti. Difatti, il concorso tra le autorità di controllo e i tribunali civili nell'applicazione del diritto sulla protezione dei dati personali avrebbe potuto causare un'invasione nella sfera delle competenze del Garante privacy «e portare a divergenze, all'interno dell'Unione, nel controllo dell'applicazione del diritto in materia di protezione dei dati».

L'obiettivo di utilizzare la violazione del GDPR anche come parametro della violazione delle regole antitrust, induce la Corte ad operare due "forzature". In primo luogo interpretare le norme del GDPR (artt. 77, 78, 79 e 80) che ammettono il reclamo del cliente interessato o di un ente legittimato (ma non di un'impresa concorrente della venditrice, che non è interessata ai sensi dell'art. 4 RGDP) nel senso di consentire anche all'impresa concorrente di poter agire in giudizio per far valere una violazione del diritto antitrust. E ciò sempre a prescindere dalla indagine in concreto dell'effettiva alterazione della dinamica concorrenziale, e sulla base dell'argomento che con l'adozione del Regolamento privacy il legislatore europeo non ha inteso procedere ad un'armonizzazione esaustiva dei mezzi di ricorso disponibili né escludere il ricorso dei concorrenti (del presunto autore di una lesione della protezione dei dati personali). Anzi dare loro la possibilità di esercitare l'inibitoria più che pregiudicare il sistema di tutela previsto dal GDPR avrebbe rafforzato il livello di protezione degli interessati (conformemente al considerando 10 del GDPR).

Con riferimento, poi, alla questione se le informazioni inserite dai clienti acquirenti dei medicinali sulla piattaforma online costituissero dati relativi alla salute di cui sarebbe vietato il trattamento ai sensi degli artt. 8, par. 1, vecchia direttiva 45/96 e 9, par. 1, RGDP, i giudici europei operano la seconda forzatura. Difatti, propendono per un'interpretazione in senso ampio della nozione «dati relativi alla salute», al fine di includervi tutti i dati che, pur non riguardando direttamente la salute dell'interessato (come le informazioni relative al nome, all'indirizzo di consegna, all'individualizzazione dei medicinali), «sono idonei a rivelare, mediante un'operazione intellettuale di raffronto o deduzione, informazioni sullo stato di salute dell'interessato ai sensi dell'art. 4, par. 1, del RGDP». Ciò in quanto l'ordine online del medicinale implica la creazione di un nesso tra il prodotto, le sue indicazioni terapeutiche o i suoi usi, e una persona fisica identificata o identificabile dagli elementi forniti. Al fine di assicurare la più ampia tutela degli interessati (come dire… *il fine giustifica i mezzi*) La Corte supera sia l'obiezione che la vendita dei medicinali online senza prescrizione potrebbe avere come destinatari soggetti diversi dall'ordinante, sia quella relativa alla scarsa accuratezza dell'informazione: poiché il trattamento dei dati, in questi casi, è idoneo a rivelare informazioni sullo stato di salute di una persona fisica a prescindere dal fatto che si tratti dell'utente o di un soggetto diverso e dall'accuratezza dell'informazione, lo stesso deve essere vietato [73].

5. – Il percorso giurisprudenziale appena tracciato ci consente di mettere in rilievo alcuni aspetti, a cominciare dal diverso ruolo attribuibile, oggi, all'informazione pubblicitaria online. Mentre, in passa-

[73] Tranne che (vedi punto 93 della sentenza) l'interessato abbia prestato il suo consenso esplicito a uno o più trattamenti di tali dati personali le cui caratteristiche e finalità specifiche gli sono state presentate in modo accurato, completo e facilmente comprensibile, oppure il trattamento sia necessario ai fini dell'assistenza sanitaria sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità.

ISSN 2281-3918/2421-2563

to, le imprese investivano una quantità eccessiva di denaro in pubblicità, oggi si assiste ad una riduzione di tale "spreco" in quanto esse orientano la comunicazione pubblicitaria secondo gli interessi dei potenziali clienti, desumendoli dalla loro frequentazione dei *social* e consultazione dei siti *web*. Le informazioni su questi interessi costituiscono, infatti, dati aventi valore economico e la loro raccolta intensiva da parte delle piattaforme social consente a queste ultime di svolgere attività di profilazione per fini commerciali, da cui si ricavano metadati che fruttano ingenti ricchezze. Si tratta, come abbiamo visto, di un nuovo modello economico che mette a dura prova le normative in materia di protezione dei dati personali, di tutela dei consumatori e di tutela della concorrenza. Le *Bigh Tech*, grazie alla massiccia raccolta di dati, possono elaborare previsioni sempre più attendibili sulle preferenze degli utenti e fornire loro prodotti/servizi personalizzati, sempre più "customizzati" e soddisfacenti al punto da "catturarli" [74], rendendo improbabile che gli utenti/consumatori abbandonino l'ecosistema digitale per cercare alternative migliori. Di fronte al "prepotere" di questi oligopoli tecnologici considerare come esaustiva e, soprattutto, esclusiva la tutela fornita dalla normativa sulla protezione dei dati personali significherebbe non tenere in considerazione che un trattamento dei suddetti dati, non necessario ai fini dell'esecuzione del contratto ed avvenuto senza il consenso libero dell'interessato [75], potrebbe ledere oltre alla privacy altri interessi dell'utente/consumatore come accade nell'ipotesi di utilizzazione a fini commerciali e pubblicitari dei suoi dati senza che l'interessato riceva un'immediata e specifica informazione al riguardo e, addirittura, venga ingannato circa la gratuità del servizio social cui si è registrato fornendo, appunto, i dati personali. Da qui la preferenza per una complementarietà di discipline (affermata come abbiamo visto sia dalla giurisprudenza italiana che da quella europea) che, lungi dal negare il primato alla normativa sulla privacy, finisce per rafforzare la tutela in essa prevista [76]. Il passaggio ulteriore, compiuto, dalla Corte di giustizia UE è stato quello di considerare la vio-

[74] Si evidenzia, in dottrina, come «l'accurata profilazione prodotta dalle tecniche di big data rafforza l'asimmetria informativa dal lato degli utenti in quanto sfrutta non solo il mito del servizio fornito "*for free*" e la scarsa consapevolezza riguardo i diritti sui propri dati ma anche i *bias* cognitivi… Grazie ai dati raccolti e nella loro disponibilità le piattaforme producono una segmentazione granulare sempre più sofisticata degli utenti e un costante perfezionamento della profilazione che può, a sua volta, influire significativamente sugli utenti stessi» e «sulla concorrenza poiché produce inerzia negli utenti scoraggiandoli dal ricercare alternative in presenza di pesanti costi di *switching*». Così L. AMMANNATI, *La circolazione dei dati: dal consumo alla produzione* in *Riv. trim. dir. econ.*, 2020, 4, 674 s., nonché, per la condizione di asimmetria informativa rafforzata in cui vengono a trovarsi i consumatori nell'era digitale, ID., *Il paradigma del consumatore nell'era digitale: consumatore digitale o digitalizzazione del consumatore?*, in *Riv. trim. dir. econ.*, 2019, 1, 8 ss.

[75] Sulla libertà e sulla validità del consenso dell'interessato al trattamento dei suoi dati importanti spunti sono desumibili dal noto caso *Orange Romania*, CGUE 11 novembre 2020, c-61/69, in *www.agendadigitale.eu*, su cui vedi, per tutti il commento di C. ANGIOLINI, *A proposito del caso* Orange Romania *deciso dalla Corte di Giustizia dell'UE: il rapporto tra contratto e consenso al trattamento dei dati personali*, in *Nuova giur. civ. comm.*, 2021, 1, 247 ss. Sulla libertà del consenso vedi, di recente, anche G. FINOCCHIARO, *Consenso al trattamento e libertà*, in S. ORLANDO (a cura di), *Libertà e liceità del consenso nel trattamento dei dati personali*, cit., 26 s. per la quale la valutazione del grado di libertà dei contraenti non si esaurisce nella sfera soggettiva della parte, ma deve considerare anche parametri esterni alla sfera del contraente. Ciò vale tanto più nell'ipotesi degli scambi in internet, che si svolgono nel breve istante di un click. Qui – si dice – «la libertà non va cercata soltanto in quel *click*, ma nei presupposti, nel contesto di quello scambio e di quella relazione», in una dimensione, cioè, contestuale.

[76] Attenta dottrina (S. PAGLIANTINI, *L'interferenza ascosa tra GDPR e diritto dei consumatori: appunti per una tassonomia*, cit., 2212 ss.) nel registrare la possibile compenetrazione del GDPR con il diritto consumeristico, nel senso di una *complementarietà incrementante* il livello di tutela e sia pure con una *postergazione gerarchica* del diritto consumeristico, mette in guardia sulle tante ombre di questo complessivo quadro di tutele *massimizzante* le garanzie per l'interessato che sia anche un consumatore. Per un verso il GDPR regola in misura alquanto limitata le conseguenze della revoca del consenso (l'obiettivo è quello di garantire i rimedi di cui agli artt. 15-22 GDPR), per altro verso, il codice del consumo – laddove di-

ISSN 2281-3918/2421-2563

lazione delle regole sulla privacy come parametro per valutare la qualità della concorrenza nel senso che «non rientra nella concorrenza basata sui meriti un'attività imprenditoriale che viola discipline legali (come quella del GDPR) pur estranee al diritto della concorrenza» [77].

Un altro profilo degno di nota è rappresentato dall'aggravata asimmetria informativa in cui versano i consumatori digitali rispetto alla controparte professionale costituita dai gestori delle piattaforme social. I primi, infatti, «generalmente non conoscono i meccanismi che consentono alle piattaforme di sfruttare la loro posizione e i dati personali raccolti come di trarre profitto dal crescente numero di accessi». Si dice che il deficit che caratterizza i consumatori sia «di natura più cognitiva che conoscitiva». Difatti, sebbene «i dati siano spesso disponibili per entrambi gli attori, soltanto l'impresa riesce ad usarli a proprio vantaggio. Si tratta delle informazioni relative alle scelte di consumo dei singoli individui (la cd. *product use information*) che l'impresa raccoglie ed elabora per il loro rilevante valore economico ma che, invece, il consumatore non è capace di valutare» [78]. Preso atto, quindi, dei limiti cognitivi in cui versano i consumatori e degli errori che contraddistinguono il loro agire la prima via percorsa è quella di una regolazione basata sull'informazione (*disclosure regulation*) dove, cioè, l'informazione diventa "strumento" di regolazione. Ciò comporta l'imposizione agli operatori di obblighi di *information disclosure* (si veda, ad es., il prospetto informativo in relazione ai servizi finanziari) o il divieto di fornire ai consumatori informazioni false o ingannevoli (come prevedono le norme del codice del consumo sulle pratiche commerciali scorrette o la disciplina sulla pubblicità ingannevole), con l'obiettivo di ridurre l'asimmetria informativa, consentendo ai destinatari dell'informazione di compiere scelte consapevoli, basate sulle loro preferenze e non alterate da strategie commerciali aggressive o carenti di informazione [79]. L'idea che bastava dotare il consumatore dell'informazione necessaria ad orientare le proprie scelte in maniera consapevole ha evidenziato segni di debolezza in mancanza di interventi necessari a rafforzare il suo apparato cognitivo [80]. Non basta ricevere le informazioni (che in quantità eccessiva possono, addirittura, danneggiare i destinatari), ma è necessario che esse siano adeguate. Il consumatore, cioè, dovrebbe avere a disposizione informazioni semplici, comprensibili e facilmente comparabili per poter effettuare scelte consapevoli ma, soprattutto, dovrebbe essere messo nelle condizioni di neutralizzare i suoi errori cognitivi [81], errori che dipendono dalla pro-

---

spone, ai sensi dell'art. 135-*noviesdecies* che, nell'ipotesi di risoluzione del contratto, il professionista rimborsa al consumatore tutti gli importi versati in esecuzione del contratto, non tiene conto dell'ipotesi di servizi digitali remunerati con il consenso al trattamento dei dati.

[77] Così M. MIDIRI, *Privacy e antitrust*, cit., 220, il quale evidenzia come la Corte di giustizia ritenga che gli abusi escludenti possano essere valutati facendo riferimento ad altri settori di diritto e richiama la sentenza *AstraZeneca c. Commissione* (CGUE 6 dicembre 2012, C-457/10, EU:C:2012:770, §98).

[78] Così L. AMMANNATI, *Il paradigma del consumatore nell'era digitale: consumatore digitale o digitalizzazione del consumatore?*, cit., 21. In generale vedi, altresì, E. BRODI, *Abitudini e preferenze di consumo. Nuove forme di disclosure per la tutela del consumatore*, in *MCR*, 2012, 394 ss., nonché A. ZOPPINI, *Contratto ed economia comportamentale*, in *Enc. dir.*, *I Tematici*, I, *Contratto*, a cura di G. d'Amico, Milano, 2021, 321 ss.

[79] L'informazione può essere oggetto di regolazione anche dal lato dell'offerta e quindi a vantaggio degli operatori. Sul punto cfr. F. DI PORTO, *L'informazione come 'oggetto' e come 'strumento' di regolazione (il caso dei mercati energetici al dettaglio)*, in *Riv. trim. dir. pubbl.*, 4/2011, 975 ss.

[80] Gli studi di economia comportamentale, infatti, evidenziano l'irrazionalità dei consumatori le cui scelte sono, spesso, frutto di percezioni inesatte o di errori cognitivi ricorrenti. Così N. RANGONE, *Errori cognitivi e scelte di regolazione*, in *Analisi giur. econ*., 2012, 1, 7 ss. In argomento cfr., altresì, F. DI PORTO, *Protezione ed* empowerment *del consumatore: profili cognitivi della regolazione*, in *www.amministrazioneincammino.luiss.it*, 4.

[81] Evidenzia A. ZOPPINI (*Contratto ed economia comportamentale*, cit., 321) come «il paradigma economico *standard* prevede che gli individui nei rispettivi processi decisionali si comportino come se tutte le informazioni fossero elaborate se-

ISSN 2281-3918/2421-2563

filazione dei suoi dati personali per cui, la tutela si sostanzia in una più rigorosa protezione degli stessi. In questa prospettiva, un ruolo fondamentale è assunto dal GDPR che prevede una serie di strumenti come l'anonimizzazione e la portabilità dei dati, ma anche il diritto alla rettifica ed all'oblio, diretti a rafforzare il controllo del singolo sui propri dati al fine di evitare una 'appropriazione' degli stessi da parte delle piattaforme. L'*empowerment* privatistico viene, poi, incrementato con i provvedimenti che aumentano il livello di trasparenza richiesto dalle transazioni concluse sui mercati online [82] e tutelano il consumatore rispetto ai contratti di fornitura di contenuti digitali o di servizi digitali che hanno come controprestazione patrimoniale non un corrispettivo in denaro ma la cessione dei dati personali degli utenti. Si tratta di strumenti che mirano ad accrescere la consapevolezza dei consumatori circa i rischi sottesi all'impiego della nuova tecnologia, ma che non tengono conto della limitata capacità di scelta del consumatore dovuta all'estensione dell'uso di 'consumatori algoritmici' (come gli assistenti digitali) che predeterminano ed influenzano la scelta di beni o servizi da parte degli utenti, senza esplicitare i criteri in base ai quali effettuano le loro scelte [83]. Una terza osservazione attiene all'uso del "quadro *data protection*" per limitare l'abuso di posizione dominante dei gestori di piattaforme di social network, considerando che la creazione di un valore economico dai trattamenti di dati personali e, in particolare, dalla combinazione di dati tra diverse sorgenti, interne ed esterne alla piattaforma, può «creare un disequilibrio nelle dinamiche competitive del mercato» [84]. Abbiamo visto come, tanto nella decisione del BKartA tedesco del 2019 che nelle successive pronunce della Corte di giustizia UE, l'utilizzo della disciplina del GDPR e, quindi, la necessità di ottenere un consenso libero e consapevole dell'interessato per poter trattare i suoi dati personali, impedisce alle piattaforme social, in assenza del consenso medesimo, di potersi giovare del vantaggio economico rappresentato dalla combinazione dei dati ivi presenti con quelli provenienti da sorgenti esterne, con conseguente possibilità che il valore economico così generato venga redistribuito tra i competitors che potrebbero aspirare a quote di mercato prima inaccessibili. L'obiettivo è quello di garantire una maggiore equità nell'accesso al mercato

condo la teoria delle probabilità (razionalità delle percezioni), le preferenze fossero stabili e precise (razionalità delle preferenze) e il processo cognitivo consistesse nella massimizzazione delle preferenze stesse (razionalità del processo). In realtà, dinanzi ai dati informativi, gli individui sono spesso soggetti ad errori cognitivi. L'ipotesi della razionalità delle percezioni si scontra con la tendenza dei soggetti a elaborare informazioni ricorrendo a procedimenti euristici capaci di generare errori sistematici rilevanti». Ma anche la razionalità delle preferenze e la razionalità del processo sono condizionate dall'informazione pubblicitaria e dalla profilazione dell'utente che orienterà le sue preferenze nella direzione dei messaggi ricevuti (e fondati sui dati che l'utente stesso aveva inserito nella piattaforma online e che hanno consentito ai gestori di essa di individuare i suoi interessi) e si convincerà della bontà delle sue scelte di acquisto senza andare alla ricerca di alternative.

[82] Si pensi alla nuova direttiva n. 2161/2019 del Parlamento Europeo e del Consiglio che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori. Questa normativa estende le regole di protezione del consumatore ai mercati digitali con particolare riguardo alle relazioni tra piattaforme e utenti finali: dal diritto ad un'informativa precontrattuale in caso di servizi *for free* alla necessaria trasparenza sulla identità della parte con cui il consumatore stipula il contratto come sui parametri che determinano il posizionamento delle offerte a seguito di una ricerca.

[83] Vedi L. AMMANNATI, *La circolazione dei dati: dal consumo alla produzione*, cit., 685

[84] Così G. D'ACQUISTO-F. PIZZETTI, *Regolamentazione dell'economia dei dati e protezione dei dati personali*, cit., 97. Gli Autori evidenziano l'esistenza di un *trade off* tra l'*empowerment* della persona ed il potere di mercato dei gestori di piattaforme social. Difatti, si dice, «meno il titolare sa a proposito della persona, minore sarà il suo potere di mercato». Nel caso deciso dal BKartA tedesco «l'abuso di posizione dominante di Facebook è infatti contrastato riducendo la possibilità che questa ha di combinare fonti diverse e dunque conoscere più approfonditamente i propri utenti, e rimettendo la combinazione di dati alla libera scelta di questi ultimi». Che i dati costituiscano non solo una risorsa economica ma anche «di potere» e che sul loro dominio «si costruiscono oligopoli alterando la leale competizione per il mercato», lo rileva anche P. STANZIONE, *La circolazione dei dati personali: persona, contratto e mercato*, a cura di A. Morace Pinelli, Pisa, 2023, 159 ss.

ISSN 2281-3918/2421-2563

da parte di tutti gli operatori economici, scardinando situazioni di abuso di posizione dominante che possono derivare non soltanto dalla quantità dei dati raccolti ed utilizzati dalle piattaforme ma anche dalla qualità di essi. Difatti, la varietà dell'osservazione può consentire la previsione di un contesto digitale nuovo in cui gli utenti potranno trovarsi e il gestore della piattaforma che riuscirà a fare tale previsione per primo potrà anticiparne le necessità (grazie all'attività di profilazione) ed acquisire vantaggi competitivi ai danni degli altri concorrenti [85]. Non sono mancate critiche – anche da parte di avveduta dottrina – circa l'improprio impiego del diritto della concorrenza per risolvere "problemi" di privacy [86]. Tuttavia, se appare "forzato" ritenere che un illecito privacy, compiuto al di fuori della sfera della concorrenza, inneschi una violazione del diritto antitrust qualora sia praticato da un'impresa dominante (in mancanza, ad es. di monopolisti che riducono la qualità dei servizi digitali o di concorrenti esclusi a causa dell'effetto di blocco innescato da pervasive esternalità di rete) è anche vero che, dopo gli ultimi interventi normativi europei, non può più negarsi il collegamento tra *consumer* e *data protection* [87], né tra quest'ultima ed il diritto Antitrust. Ciò anche per effetto della previsione, nel *Digital Market Act* (DMA) [88], di alcune disposizioni che avallano un approccio sinergico tra GDPR e disciplina antitrust [89] al fine di sopperire alla diffusa difficoltà di applicare le disposizioni antitrust ai mercati

---

[85] Oltre alla previsione di un nuovo contesto G. D'ACQUISTO-F. PIZZETTI, *Regolamentazione dell'economia dei dati e protezione dei dati personali*, cit., 103 s. evidenziano altri potenziali abusi ai danni degli utenti delle piattaforme social. Ad esempio è possibile che la previsione sia sbagliata e che la decisione che ne consegue sia penalizzante e discriminatoria e ciò non soltanto per colpa dell'autore dell'algoritmo impiegato per fare le previsioni ma anche per il semplice fatto di appartenere ad una minoranza che non si comporta come la maggioranza. Ma anche laddove la previsione sul comportamento futuro di una persona di cui non si conoscono abitudini e preferenze fosse azzeccata si corre il rischio che chi effettua il trattamento predittivo potrebbe sfruttare la previsione per avvantaggiarsene «ad esempio con forme di *value pricing* capaci di estrarre per intera la nostra disponibilità di spesa».

[86] Si vedano, in particolare, R. PARDOLESI-R. VAN DER BERGH-F. WEBER, *Facebook e i peccati da "Konditionenmissbrauch"*, in *MCR*, 3/2020, 512 ss.; P. MANZINI, *Antitrust e privacy: la strana coppia*, in *Quaderni AISDUE*, in *www.aisdue.eu*, sezione articoli, n. 10, 15 settembre 2023, 196 ss., nonché G. OLIVIERI, *Sulle "relazioni pericolose" fra antitrust e privacy nei mercati digitali*, in *Rivista Osserv. dir. comm*., fascicolo speciale, 2021, 359 ss.

[87] Scrive, infatti, S. PAGLIANTINI, *L'interferenza ascosa tra GDPR e diritto dei consumatori: appunti per una tassonomia*, cit., 2219 che «l'interazione tra *consumer* e *data protection* conosce adesso pure l'epifania di un GDPR trasformato in *asset* della tutela consumeristica: come accade, risaputamente, con la Dir. 2020/1828, se è vero che le azioni rappresentative a tutela degli interessi collettivi dei consumatori sono esercitabili anche in caso di infrazione alle discipline sulla protezione dei dati personali. Siamo dalle parti, pur se l'art. 3 della 2020/1828 è tutt'altro che perspicuo sul piano definitorio, di una traiettoria rimediale che vede la *consumer law* azionarsi *a valle* di una violazione *a monte* del GDPR (art. 2, par. 1 ed allegato I, n. 56), il cui articolato è così trasformato in elemento di una strategia – "onnicomprensiva" – di contrasto integrata (art. 140 ter, 2° comma, c. cons.)».

[88] Ovvero il regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), in GUUE del 12 ottobre 2022 L265.

[89] Vedi, in particolare, il par. 2 dell'art. 5 DMA che vieta ai *gatekeeper* (cioè ai fornitori di almeno un servizio di piattaforma base come, ad es., quello di social network) di trattare in modo combinato i dati personali dei suoi utenti, a meno che sia stata loro presentata una scelta specifica ed essi abbiano dato un valido consenso ai sensi del GDPR. La previsione di specifici obblighi e divieti per i gatekeeper, come quelli contenuti negli artt. 5, 6 e 7 DMA derivano dalla constatazione (del legislatore europeo) che alcuni fattori dimensionali delle imprese operanti nei mercati digitali possono generare barriere all'entrata così significative da minacciare in modo irreparabile la competitività del sistema (cfr. M. SCIALDONE, *Il procedimento di designazione dei gatekeeper*, in L. BOLOGNANI-E. PELINO-M. SCIALDONE (a cura di), *Digital Service Act e Digital Market Act. Definizioni e prime applicazioni dei nuovi regolamenti europei*, Milano, 2023, 301). Gli obblighi elencati nel suddetto art. 5 DMA sono specificati nei considerando 36 e 37 e da una lettura complessiva di queste disposizioni è possibile desumere che l'interesse tutelato dal DMA non è tanto l'autodeterminazione informativa degli utenti/interessati (a presidio del quale sono poste le norme del GDPR) quanto quello della contendibilità dei servizi digitali, interesse che può essere pre-

ISSN 2281-3918/2421-2563

digitali. Il DMA, in particolare, mirerebbe a prevenire gli illeciti concorrenziali in questi mercati dove l'applicazione delle norme antitrust tradizionali (come la nullità delle intese o le sanzioni dell'abuso di posizione dominante) oltre ad essere eventuale è successiva al verificarsi dell'illecito e, pertanto, inidonea a scongiurare il persistere di condotte nocivi agli interessi di consumatori e concorrenti [90]. Una quarta ed ultima osservazione concerne il ruolo del consenso dell'interessato e la perdita della sua centralità [91] nell'ipotesi di trattamenti massivi di Big Data. In questo caso, infatti, si assiste ad una perdita di controllo sul dato da parte dell'interessato dovuta ad una molteplicità di fattori. «Dinanzi al fenomeno dei big data l'utente … non ha a che fare con dati dotati di immediata attitudine comunicativa e pertanto egli comprende meno di quanto quei dati possano dire di sé ai professionisti del settore. Una disattenta prestazione del consenso è, allora, frequentemente incoraggiata dalla scarsa dimestichezza con i servizi della società dell'informazione o dalla naturale inaccessibilità del navigatore medio alla

giudicato dal comportamento scorretto del gatekeeper. La violazione delle norme del GDPR, in altri termini, diventa un importante indizio di una condotta sleale del gatekeeper e, quindi, potenzialmente lesiva anche della concorrenza. Tuttavia, per quanto detto in precedenza, la connessione privacy – antitrust non può essere letta anche al contrario nel senso che una maggiore *policy privacy* non assicura automaticamente il rispetto del diritto antitrust, anzi spesso può essere lo strumento con cui si realizzano strategie anticoncorrenziali come nell'esaminato caso *Apple ATT.*

[90] Sul punto, cfr. P. MANZINI, *Il Digital Market specifica che «l'alternativa Act decodificato*, in AA.VV., *Unione Europea 2020. I dodici mesi che hanno segnato l'integrazione europea*, Milano, 2021, 324.

[91] Sulla perdita centralità del consenso dell'interessato si è discusso molto in dottrina per la presenza di non poche ipotesi in cui la liceità del trattamento viene fondata su basi giuridiche diverse dal consenso (vedi art. 6, par. 1, lett. da *b*) ad *f*) del GDPR) o viene riconosciuta anche al trattamento che persegue finalità diverse, sebbene compatibili con quelle che hanno determinato la raccolta dei dati (vedi art. 6, par. 4, lett. da *a* ad *e*, GDPR). Tuttavia, sono prevalenti le disposizioni che assegnano un ruolo centrale al consenso dell'interessato nella valutazione della liceità del trattamento (vedi art. 9, par. 2, lett. *a* e art. 7 GDPR). Così A. PURPURA, *Il consenso nel mercato dei dati personali. Considerazioni al tempo dei Big Data*, in questa *Rivista*, 4/2022, 901 ss. L'A. si interroga anche sulla natura giuridica del consenso richiesto quale base giuridica del trattamento e tra le due letture (consenso come mero atto autorizzatorio alla stregua del consenso previsto dall'art. 50 c.p. e consenso dal valore negoziale), propende per la lettura negoziale di esso con la precisazione che, data la particolare natura del bene-dato personale, il consenso al trattamento non potrà essere né traslativo, né definitivo. Più in generale, la dottrina concorda nel ritenere che, nel mercato unico digitale europeo i dati personali non costituiscono né diritti della persona *tout court*, né beni appropriabili in senso tradizionale ed è per questo che la loro tutela non può perfettamente coincidere né con il diritto di proprietà, né con i diritti della personalità, ma si tratta di una tutela flessibile che assume elementi sia del primo che dei secondi. In dottrina (G. PIGNATARO, *Circolazione dei dati tra modelli proprietari e contrattuali*, in *www.medialaws.it*, 2/2024, 25) si afferma che «il diritto di accesso ai dati personali può prescindere dal consenso e comunque non conferisce mai un pieno potere di gestione. Può prescindere dal consenso, se rappresenta una delle possibili condizioni di liceità del trattamento dei dati; ne limita la gestione perché, anche in presenza di un consenso, il titolare o il responsabile del trattamento dei dati non è mai libero di gestirli a piacimento, se le finalità dichiarate rappresentano un limite intrinseco funzionale. Il regime delle responsabilità, modulato secondo il principio della *data protection by design e by default*, fa gravare su costoro l'obbligo di adottare già in fase di progettazione le tecnologie idonee a garantire la privacy e la sicurezza degli utenti (*data protection by design*) nonché l'utilizzo di tecniche per un approccio selettivo dei dati, limitato ai soli necessari per migliorare il servizio e la sicurezza del prodotto (*data protection by default*), mentre il soggetto cui i dati si riferiscono non ne perde mai la titolarità, che legittima il potere di controllo sul loro corretto trattamento». L'esclusione di un modello proprietario e di un modello esclusivamente personalista dei dati personali si giustifica anche in considerazione della circostanza, sempre più frequente, che i Big Data prodotti dalle attività di profilazione possono essere costituiti da dati personali e da dati non personali (non sempre facilmente distinguibili dai primi) la cui disciplina, oggi contenuta nel *Data Act* (regolamento UE 2023/2854), ne consente la circolazione, mediante contratto. Si dice, infatti, che «se il dato personale è oggetto di un trattamento correlato ad un'operazione economica, è elemento di un'operazione di scambio patrimoniale, … sarà inevitabilmente coinvolto nella vicenda della condivisione dei dati come disciplinata dal *Data Act*», ferma restando l'impossibilità per questo Regolamento – e sarebbe questa l'unica limitazione individuabile nella sua disciplina rispetto alla circolazione contrattuale dei dati personali – di «costituire una base giuridica per la raccolta e la generazione di dati personali da parte del titolare dei dati». (Così V. RICCIUTO, *Economia e mercato dei dati. Note a margine del c.d.* Data Act, in *Accademia*, 6/2024, 488).

ISSN 2281-3918/2421-2563

comprensione di meccanismi dall'elevato livello di complessità o sofisticazione o, ancora, dalla sensazione che la circolazione in forma aggregata di una vasta mole di dati riesca a maggiorare i vantaggi dei servizi offerti rispetto ai rischi di nocumento alla propria persona» [92]. A ciò si aggiungono la difficoltà di revocare il consenso (prima prestato) e la depersonalizzazione del dato attraverso le tecniche di anonimizzazione [93] e pseudonomizzazione [94] che costituiscono strumenti di alterazione della capacità identificativa del dato con la conseguenza che il controllo su di esso trasla dalle mani dell'interessato a quelle dei *data players*. Da qui l'esigenza di una tutela che affianchi alla valorizzazione del consenso ed alla prospettiva di tutela esclusivamente individuale (che emerge dal GDPR) anche strumenti di public enforcement, come quelli previsti dalla disciplina sulle pratiche commerciali scorrette e dalla disciplina della concorrenza, che mettono in gioco una tutela di tipo amministrativo, affidata all'AGCM (ai sensi dell'art. 66 codice del consumo), sicuramente più efficace laddove dispone non soltanto sanzioni pecuniarie ma anche la pubblicazione, a spese del gestore della piattaforma online che ha trattato illecitamente i dati personali degli utenti, di una dichiarazione rettificativa, ai sensi dell'art. 27, comma 8, cod. cons., in cui si dà atto della scorrettezza compiuta, dichiarazione che viene pubblicata sull'home page del sito internet aziendale e sulle app aziendali, in posizione tale da consentire un'immediata visibilità agli utenti del trattamento illecito commesso [95]. Una dichiarazione di tal fatta, visibile da un pubblico illimitato di utenti, è idonea a danneggiare fortemente l'immagine della piattaforma scorretta e, probabilmente, rappresenta un deterrente maggiore anche rispetto ad ingenti sanzioni economiche. In ipotesi di danni cagionati da trattamenti massivi o per usi secondari, oltre a strumenti giuridici di tipo aquiliano o contrattuale potrebbero giovare anche regole che amplino l'*accountability* [96] del titolare del trattamento il quale dovrebbe essere spinto a minimizzare i rischi di

[92] Così A. PURPURA, *op. cit.*, 896, cui si riferiscono i virgolettati.

[93] Si priva definitivamente il dato personale della sua capacità identificativa, ad esempio generando distorsioni o alterazioni tali da renderlo non riconducibile all'utente e, quindi, inqualificabile per il GDPR come dato personale da tutelare.

[94] Tale tecnica permette di mantenere la corrispondenza del dato pseudonomizzato con quello originario, grazie all'utilizzo di informazioni aggiuntive che, pur modificando il dato, non escludono la sua riconducibilità all'interessato né la sua qualifica di dato personale ai sensi del GDPR, con conseguente possibilità di applicare la disciplina sulla *data protection*.

[95] Ad esempio, nel Provvedimento n. 27432 dell'AGCM (PS 11112 – *Facebook – Condivisione dati con terzi*), l'Autorità garante ha disposto la pubblicazione da parte di Facebook Inc. e Facebook Ireland Ltd. della seguente dichiarazione rettificativa: «Le società Facebook Inc. e Facebook Ireland Ltd. Non hanno informato adeguatamente e immediatamente i consumatori, in fase di attivazione dell'account, dell'attività di raccolta, con intento commerciale, dei dati da loro forniti. In tal modo hanno indotto i consumatori a registrarsi sulla Piattaforma Facebook, enfatizzando anche la gratuità del servizio. Inoltre, hanno esercitato un indebito condizionamento nei confronti dei consumatori registrati, i quali subiscono, senza espresso e preventivo consenso, la trasmissione e l'uso da parte di Facebook e di terzi, per finalità commerciali, dei dati che li riguardano. L'indebito condizionamento deriva dalla preselezione da parte di Facebook delle opzioni sul consenso alla trasmissione dei propri dati da/a terzi, attraverso in particolare l'automatica attivazione della funzione "Piattaforma attiva", unitamente alla prospettazione, a seguito della disattivazione di tale Piattaforma, di rilevanti limitazioni di fruibilità del social network e dei siti web/app di terzi, più ampie e pervasive rispetto a quelle effettivamente applicate. Tali pratiche sono state valutate scorrette, ai sensi degli artt. 21, 22, 24 e 25 del Decreto Legislativo, n. 206/2005 (Codice del Consumo). L'Autorità ha disposto la pubblicazione della presente dichiarazione rettificativa ai sensi dell'art. 27, comma 8, del Codice del Consumo. (Provvedimento adottato nell'adunanza del 29 novembre 2018 e disponibile sul sito www.agcm.it)».

[96] Principio che assume grandissimo rilievo già nel GDPR, obbligando tutti i responsabili del trattamento ad attuare misure e procedure per la protezione del dato, nonché per la dimostrazione della liceità del trattamento (vedi artt. 24 e 32). In dottrina ciò è stato messo bene in evidenza, tra gli altri, da G. FINOCCHIARO, *Il principio di accountability*, in *GDPR tra novità e discontinuità*, a cura di R. Caterina, in *Giur. it.*, 12/2019, 2778; R. CATERINA, *Novità e discontinuità nel Regolamento generale sulla protezione dei dati personali*, sempre in *GDPR tra novità e discontinuità*, cit., 2777, nonché da M.G. STANZIONE, *La protezione dei dati personali tra «consumerizzazione» della privacy e principio di accountability*, in *Comparazione dir. civ.*, 1/2022, 1 ss.

ISSN 2281-3918/2421-2563

perdita di controllo dei dati da parte dell'utente. Si tratta di un approccio basato su strumenti preventivi di responsabilizzazione che si allinea alle scelte operate dal legislatore europeo in tutta una serie di provvedimenti (*Digital Market Act, Digital Services Act*[97], *AI ACT*[98]) volti a regolare il fenomeno dell'economia digitale. Senza contare che le disposizioni anche sanzionatorie previste nei Regolamenti sui mercati e sui servizi digitali possono essere suscettibili di applicazione diretta qualora il gestore della piattaforma online (qualificabile come gatekeeper) ponga in essere una pratica commerciale scorretta a danno sia degli utenti (dei cui dati traggono vantaggi economici) che delle imprese concorrenti.

[97] Si tratta del regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), consultabile su GUUE del 27 ottobre 2022 L277.

[98] Noto anche come Legge sull'IA (regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

ISSN 2281-3918/2421-2563