

Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*

Shaira Thobani

Abstract

Il diffondersi della prassi di offrire servizi senza richiedere in cambio un corrispettivo in denaro ma subordinando l'erogazione del servizio alla prestazione del consenso al trattamento dei dati personali degli utenti impone di verificare la liceità di tali operazioni e, dunque, della possibilità di usare i dati personali come moneta corrente per accedere a beni o servizi. La questione rileva sotto profili differenti, in quanto chi accede a un servizio acconsentendo al trattamento dei propri dati è sia un utente-consumatore, sia un "interessato" (soggetto, cioè, cui i dati si riferiscono). Il saggio intende dunque analizzare come le norme a tutela dei consumatori, da un lato, e quelle in materia di protezione dei dati personali, dall'altro, affrontino la questione della legittimità del mercato dei dati personali, giungendo alla conclusione che mentre le prime si limitano a indicare come tale scambio debba essere attuato, sono le seconde a stabilire i criteri per verificarne la legittimità sostanziale.

The prevailing business model of offering services "for free" asking the users to consent to the processing of their personal data raises the question of the legitimacy of the practice of using personal data as currency to have access to goods or services. The issue is relevant under different perspectives, as those who access a service consenting to the processing of their personal data are both consumers and data subjects. The essay therefore intends to analyse how consumer protection rules, on the one hand, and data protection regulation, on the other, tackle the issue of the legitimacy of a personal data market. As the article tries to prove, while consumer protection regulates the conditions of such an exchange, it is data protection rules that regulate the merits of its legitimacy.

Sommario

1. Introduzione. – 2. Profili di tutela dell'utente. – 3. I dati personali come controprestazione. – 4. Profili di tutela dell'interessato. – 5. Considerazioni conclusive.

Keywords

Privacy; Dati personali; Tutela dei consumatori; GDPR; Operazioni di tying

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco"

1. Introduzione

È nota la diffusione del *business model* di offrire servizi gratuitamente, senza cioè la previsione di un corrispettivo in denaro ma previa acquisizione del consenso al trattamento dei dati personali degli utenti. Si tratta di un modello estremamente diffuso nei rapporti online (anche se non ad essi limitato), sviluppatosi grazie all'evoluzione delle nuove tecnologie che rendono possibili sempre più pervasive e sofisticate tecniche di raccolta, monitoraggio e sfruttamento dei dati personali. L'erogazione di beni e servizi rappresenta infatti una preziosa occasione per accedere alle potenzialità economiche dei c.d. big data¹. Da un lato, l'uso dei servizi da parte degli utenti genera di per sé dati (sulle preferenze e i comportamenti degli utenti, quali, ad esempio, le abitudini di consumo) il cui sfruttamento dà luogo a utilità economiche, dall'altro l'offerta di un bene o servizio rappresenta l'occasione per chiedere agli utenti di comunicare essi stessi alcune informazioni che li riguardano. È dunque frequente che, in sede di accesso a un servizio, sia richiesto all'utente di prestare il consenso al trattamento dei dati personali per fini ulteriori (non necessari all'erogazione del servizio)² e che tale consenso sia posto come condizione necessaria per accedere al servizio: si tratta delle operazioni c.d. di *tying*. Ha così luogo uno scambio tra il servizio e i dati personali, che costituiscono, almeno di fatto, il corrispettivo per accedere alla controprestazione³.

La prassi in questione genera seri interrogativi, riguardanti innanzitutto la liceità dello scambio dei dati personali con un servizio. È ammesso un mercato dei dati personali⁴? I profili che si intrecciano e gli interessi coinvolti sono molteplici, venendo in considerazione la doppia posizione rivestita da chi richiede il servizio, quale utente, da un lato,

¹ Il valore economico dei dati personali è indubbio, nonostante permangano seri dubbi su quale sia il modo più accurato per misurarlo. V., ad esempio, lo studio effettuato dalla Organisation for Economic Co-Operation and Development, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers No. 220, 2013. Sulle modalità di quantificazione del valore economico dei dati personali, v. anche G. Malgieri, B. Custers, *Pricing privacy – the right to know the value of your personal data*, in *Computer Law & Security Review*, 34, 2017, 294-297. Cfr. in proposito F.G. Viterbo, *Freedom of contract and the commercial value of personal data*, in *Contratto e impresa Europa*, 2, 2016, 606-607.

² I dati raccolti in sede di erogazione di un servizio sono di diverso genere. Mentre alcuni di questi dati sono necessari per l'erogazione del servizio stesso (così, l'indirizzo dell'utente è necessario qualora si chieda la consegna di un bene acquistato a distanza), altri sono invece richiesti per finalità ulteriori, quali scopi di profilazione e marketing. Chiaramente, solo questi ultimi costituiscono il "corrispettivo" del servizio.

³ Sulla possibilità di considerare i dati personali (*rectius* il consenso al trattamento dei dati personali) come oggetto di una prestazione e sul conseguente nesso di corresponsività tra tale consenso e l'accesso al bene o servizio per cui il consenso è richiesto v. C. Langhanke, M. Schmidt-Kessel, *Consumer data as consideration*, in *Journal of European Consumer and Market Law*, 2015, 6, 218 ss.; A. De Franceschi, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, 67 ss.; A. Metzger, *Data as Counter-Performance: What Rights and Duties do Parties Have?*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8, 2017, 1 ss.; G. Resta, V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Rivista trimestrale di diritto e procedura civile*, 2018, 436 ss.; S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018, 160 ss.

⁴ Si fa riferimento al mercato per così dire primario dei dati, nel senso di mercato in cui sono gli interessati stessi a immettere i dati nei circuiti di circolazione. Diverso è invece il discorso con riguardo al mercato secondario dei dati, in cui i titolari del trattamento, una volta raccolti i dati, li fanno a loro volta circolare. In generale, sui problemi legati al mercato dei dati v. V. Zeno-Zencovich, *Do "Data Markets"*

e quale interessato (persona, cioè, a cui si riferiscono i dati), dall'altro. Non bisogna poi dimenticare la dimensione di massa del fenomeno in esame, per cui la liceità del singolo scambio andrà valutata alla luce dei più generali interessi coinvolti da rapporti di tipo seriale.

2. Profili di tutela dell'utente

Chi accede a un bene o servizio è innanzitutto un utente. Lo sviluppo, di fatto, di un mercato dei dati personali impone dunque di prendere in considerazione gli interessi legati alla tutela del mercato. La questione si è inizialmente posta come un problema di trasparenza dell'offerta di beni o servizi pubblicizzati come gratuiti ma in realtà prestati in cambio del consenso al trattamento dei dati personali⁵.

In tali termini essa è stata oggetto di alcuni provvedimenti dell'Autorità garante della concorrenza e del mercato, che ha sanzionato la pratica di pubblicizzare un servizio come gratuito laddove si richiedeva il consenso dell'utente al trattamento dei propri dati per l'invio di e-mail pubblicitarie. L'Autorità è giunta a configurare «l'obbligo in capo al destinatario di tollerare l'invio per posta elettronica di messaggi pubblicitari, “profilati” sulla base del proprio utilizzo della rete via Internet» come «una vera e propria prestazione passiva», non «indifferente ai fini della valutazione della convenienza dell'offerta». Ne deriva che i messaggi pubblicitari in questione costituiscono pubblicità ingannevole considerata «[l]a circostanza che tali condizioni non [sono] immediatamente e chiaramente percepibili, in quanto, nel caso di specie, sono contenute nella finestra di testo che riporta le condizioni generali di contratto, risulta idonea a indurre i consumatori in errore, potendo peraltro pregiudicarne indebitamente il comportamento economico»⁶. L'Autorità è più recentemente tornata sulla questione, sanzionando come pratica commerciale scorretta (in particolare, aggressiva) la condotta di WhatsApp, consistente nell'aver fatto credere ai propri utenti che sarebbe stato impossibile proseguire nell'uso dell'applicazione se non avessero accettato la condivisione dei dati con Facebook⁷. Nel motivare la propria decisione, l'Autorità preliminarmente

Exist?, in *questa Rivista*, 1, 2019, 22 ss.

⁵ Segnala come si tratti della prospettiva emersa nell'ordinamento statunitense M. Graziadei, *Collusioni transatlantiche: consenso e contratto nel trattamento dei dati personali*, in F. Di Ciommo, O. Troiano (a cura di), *Giurisprudenza e autorità indipendenti nell'epoca del diritto liquido. Studi in onore di Roberto Pardolesi*, Piacenza, 2018, 367. Sulla possibile scorrettezza delle pratiche in questione v. A. De Franceschi, *op. cit.*, 101 ss. Sull'applicabilità della normativa in materia di pratiche commerciali scorrette ai casi di raccolta di dati personali v. anche M. Rhoen, *Beyond consent: improving data protection through consumer protection law*, in *Internet Policy Review*, 5, 2016, 7-8 (il quale accenna anche alla possibilità di applicare le norme in materia di clausole vessatorie); N. van Eijk, C.J. Hoofnagle, E. Kannekens, *Unfair Commercial Practices: A Complementary Approach to Privacy Protection*, in *European Data Protection Law Review*, 3, 2017, 334, i quali svolgono l'analisi con riguardo sia all'ordinamento statunitense che a quello europeo; C. Goanta, S. Mulders, *'Move Fast and Break Things': Unfair Commercial Practices and Consent on Social Media*, in *Journal of European Consumer and Market Law*, 4, 2019, 141 ss. Sull'intreccio dei diversi piani di tutela, dei consumatori da un lato, e degli interessati dall'altro, v. G. Resta, *Digital platforms and the law: contested issues*, in *questa Rivista*, 1, 2018, 245 ss.

⁶ Prov. nn. 10276, 10277, 10278 e 10279, 20 dicembre 2001, in *Boll. sett. AGCM* n. 51-52, 7 gennaio 2002, 148-165.

⁷ Autorità garante della concorrenza e del mercato, provv. *WhatsApp – Trasferimento dati a Facebook*, 11

evidenzia che «[i]l patrimonio informativo costituito dai dati degli utenti di WhatsApp, utilizzato per la profilazione degli utenti medesimi a uso commerciale e per finalità di *marketing*, acquista, proprio in ragione di tale uso, un valore economico idoneo, dunque, a configurare l'esistenza di un rapporto di consumo tra il Professionista e l'utente». Accertata la sussistenza di un rapporto di consumo⁸, la natura aggressiva determinante l'illiceità della condotta del professionista è stata ravvisata non tanto nel non aver consentito agli utenti di negare il consenso al trattamento dei propri dati, quanto nel non aver loro prospettato in maniera chiara e immediata la possibilità di non prestare il consenso, che in realtà era offerta seppure solo in termini di *opt-out*. Simili valutazioni sono state effettuate dall'Autorità in un successivo caso riguardante condotte poste in essere da Facebook⁹. In particolare il Garante, premessa la sussistenza di un rapporto di consumo in ragione del valore economico dei dati raccolti dal gestore del social network, ha sanzionato come pratica commerciale ingannevole la condotta di non informare chiaramente gli utenti in fase di registrazione al servizio delle finalità remunerative dello stesso e, anzi, di pubblicizzarne la "gratuità"; e come pratica commerciale aggressiva quella di preselezionare l'opzione di condivisione dei dati prospettando agli utenti in caso di deselezione rilevanti limitazioni nella fruizione del servizio, maggiori rispetto a quelle effettivamente applicate.

Anche la Commissione Europea si è interessata del tema, affermando che la violazione della normativa in materia di dati personali può rilevare ai fini della valutazione del carattere sleale di una pratica commerciale sotto il particolare profilo della trasparenza. Infatti, in ragione del «valore economico *de facto*» assunto dai dati personali, la pratica di non comunicare ai consumatori che i dati che questi ultimi sono tenuti a fornire per accedere al servizio saranno usati a fini commerciali «può essere considerata un'omissione ingannevole di informazioni rilevanti»¹⁰.

maggio 2017, n. 26597, su cui v. G. Giannone Codiglione, *I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la "consumerizzazione della privacy"*, in *Diritto dell'informazione e dell'informatica*, 2, 2017, 418 ss. Sulla rilevanza della necessità di fornire un'informazione completa e trasparente in merito al trattamento dei dati personali anche ai fini della valutazione sulla correttezza delle pratiche commerciali, v. anche Tar Lazio, sez. I, 11 aprile 2018, n. 5043.

⁸ Dubbi su tale sussistenza (e, dunque, sull'applicabilità delle norme a tutela dei consumatori) potrebbero sollevarsi sulla base della supposta gratuità dei rapporti in questione. In favore dell'applicabilità della disciplina consumeristica a tali rapporti v. G. De Nova, *I contratti per l'accesso ad Internet*, in *Annali italiani del diritto d'autore, della cultura e dello spettacolo*, 1, 1996, 42-43; F. Delfini, *I contratti dei consumatori e Internet*, in C. Vaccà (a cura di), *Consumatori, contratti, conflittualità. Diritti individuali, interessi diffusi e mezzi di tutela*, Milano, 2000, 337; S.F. Bonetti, *La tutela dei consumatori nei contratti gratuiti di accesso ad internet: i contratti dei consumatori e la privacy tra fattispecie giuridiche e modelli contrattuali italiani e statunitensi*, in *Diritto dell'informazione e dell'informatica*, 6, 2002, 1129 ss.; P. Sammarco, *Le clausole contrattuali di esonero e trasferimento della responsabilità inserite nei termini d'uso dei servizi del web 2.0*, in *Diritto dell'informazione e dell'informatica*, 4-5, 2010, 640; F. Agnino, *Fino a che punto è possibile disporre contrattualmente dei propri diritti? (Vedi contratto FB)*, in *Giurisprudenza di merito*, 12, 2012, 2559. L'orientamento prevalente in sede europea è comunque quello di considerare applicabili le norme a tutela dei consumatori, a nulla rilevando la supposta "gratuità" dei contratti in questione, smentita peraltro dal valore economico dei dati personali raccolti.

⁹ Autorità garante della concorrenza e del mercato, provv. *Facebook – condivisione dati con terzi*, 29 novembre 2018, n. 27432. Si noti che, stando a quanto afferma l'Autorità, la qualifica delle condotte in esame come aggressive discende non tanto dal far seguire conseguenze negative alla revoca del consenso al trattamento, quanto (oltre che dal preselezionare l'opzione della prestazione del consenso) dal prospettare conseguenze negative maggiori di quelle effettivamente applicate.

¹⁰ Commissione europea, *Orientamenti per l'attuazione/applicazione della direttiva 2005/29/CE relativa alle*

L'esigenza di garantire la trasparenza delle operazioni di mercato impone quindi di riconoscere e rendere esplicito il nesso sinallagmatico che, almeno di fatto, si instaura tra la fornitura di un bene o di un servizio e la prestazione del consenso al trattamento dei dati personali da parte degli utenti. È dunque una pratica commerciale scorretta dichiarare che il servizio è “gratuito”, quando in realtà l'utente è costretto, per accedere al servizio, a “pagare” acconsentendo al trattamento dei propri dati¹¹. È però anche una pratica commerciale scorretta offrire un servizio prevedendo per l'utente la scelta se acconsentire o meno al trattamento dei propri dati ma senza rendere tale possibilità chiara ed esplicita.

Sempre con riguardo alla tutela del mercato, l'esplicitazione del nesso tra fornitura del servizio e prestazione del consenso al trattamento non solo è volta a garantire la trasparenza delle operazioni di mercato al fine di evitare pratiche commerciali scorrette, ma conduce anche a riconoscere all'utente le stesse tutele predisposte in favore dei consumatori. Ne è una chiara dimostrazione la recente direttiva relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali¹², che prende direttamente in considerazione la prassi di scambiare beni o servizi con dati personali. La direttiva è infatti applicabile non solo qualora il contenuto o servizio digitale sia fornito al consumatore in cambio di un prezzo, ma anche «nel caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico» (art. 3, par. 1). Lo scopo è quello di parificare i rimedi a tutela dei consumatori a prescindere da come il servizio sia stato “pagato” (se in denaro o in dati personali)¹³.

pratiche commerciali sleali, 25 maggio 2016, 28.

¹¹ Il caso può ricordare quello dei mercati c.d. a due versanti, definiti, in via approssimativa e semplificata, come quei mercati caratterizzati dalla presenza di una piattaforma che mette in comunicazione due diversi gruppi di utenti, i quali traggono beneficio proprio da tale intermediazione. La nozione di *two-sided markets*, (messa a punto da J.C. Rochet, J. Tirole, *Platform competition in two-sided markets*, in *Journal of the European Economic Association*, 1(4), 2003, 990 ss.) è stata prevalentemente utilizzata in ambito antitrust; essa, tuttavia, è anche servita a chiarire i vantaggi che i gestori delle piattaforme ottengono dal fornire servizi apparentemente gratuiti. Che il mercato sia a due versanti non comporta tuttavia necessariamente che vi sia un rapporto di corrispettività (almeno in senso giuridico) tra l'intermediario e gli utenti di uno dei due versanti; a tal fine è infatti necessario che anche gli utenti si sottopongano a un sacrificio che sia tale in termini giuridici. Nel caso che ci interessa, l'utente non ha un ruolo meramente passivo (come nel caso degli utenti nei mercati a due versanti, si pensi agli spettatori di programmi televisivi gratuiti in cui vengono trasmessi spot pubblicitari), ma gli viene richiesta una vera e propria prestazione, ovvero il consenso al trattamento dei dati, che (in mancanza di un'altra condizione di liceità) non potrebbe essere posto in essere. In tema cfr. G.A.M. Bellomo, *“There ain't no such thing as a free lunch”. Una riflessione sui meccanismi di mercato dell'economia digitale e sull'effettività delle tutele esistenti*, in *Concorrenza e mercato*, 1, 2016, 215, che sottolinea la differenza delle piattaforme della *digital economy* rispetto ai tradizionali mercati a due versanti, in quanto nelle prime gli utenti non svolgono solo un ruolo passivo (di pubblico per gli inserzionisti), ma generano attivamente dati che vengono poi utilizzati per trarne valore. Cfr. anche W. Virga, *Inadempimento di contratto e sanzioni private nei social network*, in *Annali italiani del diritto d'autore, della cultura e dello spettacolo*, 1, 2011, 232.

¹² Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali.

¹³ V. infatti il considerando n. (24), in cui si precisa che «[o]ltre a riconoscere appieno che la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce, la presente direttiva dovrebbe garantire che i consumatori abbiano diritto a rimedi contrattuali, nell'ambito di tali modelli commerciali». La precisazione iniziale in merito alla natura di diritto fondamentale del diritto alla protezione dei dati personali nasce in risposta alle osservazioni del Garante

Sul punto è interessante segnalare che l’Autorità Garante della concorrenza e del mercato, nel dichiarare la vessatorietà di alcune clausole previste nelle condizioni di utilizzo di WhatsApp, ha richiamato a sostegno della soluzione adottata «l’ormai consolidato orientamento della Commissione europea volto a riconoscere la natura di controprestazione non pecuniaria dei dati degli utenti del *social media*, sia in sede di tutela del consumatore che in sede di valutazione delle concentrazioni tra imprese, valore economico idoneo, dunque, a configurare l’esistenza di un rapporto di consumo tra il Professionista e l’utente»¹⁴. Se ne ricava dunque che la prestazione del consenso al trattamento dei dati, laddove prevista nell’ambito della fornitura di un bene o servizio, deve essere presa in considerazione al fine di applicare la disciplina a tutela dei consumatori.

Sotto questo profilo gli interessi in gioco nell’apprezzare la liceità del mercato dei dati personali sono quelli degli utenti/consumatori a ricevere informazioni trasparenti sulle operazioni di mercato che pongono in essere e ad essere tutelati in maniera adeguata in caso di inadempimento della controparte. Non pare, tuttavia, che le norme a tutela dei consumatori possano regolare nel merito lo scambio dei dati personali; non sembra, cioè, che esse possano perimetrare la misura in cui è lecito il mercato dei dati personali, una volta che ne sia stata assicurata la trasparenza.

Un controllo sul merito potrebbe aversi se il diritto dei consumi autorizzasse a considerare di per sé vessatoria la clausola che richiede a chi voglia accedere a un bene o servizio di prestare il consenso al trattamento dei dati. In tal modo si porrebbe infatti un divieto a queste operazioni. Tale soluzione non sembra però potersi sostenere. Come noto, ai sensi dell’art. 34, c. 2 cod. cons., il contenuto economico dei contratti tra professionisti e consumatori non è oggetto di valutazione, purché le condizioni contrattuali siano espresse in maniera chiara e trasparente. Il confine tra squilibrio economico e normativo dei contratti tra professionisti e consumatori costituisce un tema delicato e complesso¹⁵. Basti qui notare che qualificare la prestazione del consenso al trattamento dei dati personali come controprestazione per accedere a un bene o servizio fa propendere nettamente verso una sua ricomprensione nel contenuto economico dell’affare, rispetto a cui la legge consente di effettuare un sindacato di trasparenza ma non di merito¹⁶. Peraltro, la circostanza che una stessa direttiva europea (quella in tema di fornitura di contenuto o servizi digitali) contempli la possibilità che a fronte dell’accesso a un bene o servizio il consumatore paghi un corrispettivo in denaro o

europeo per la protezione dei dati personali, che ha contestato la qualifica dei dati personali come controprestazione: *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for supply of digital content*, 14 marzo 2017, su cui vedi *infra* nel testo in sede di conclusioni.

¹⁴ Prov. 11 maggio 2017, n. 26596, §§ 62-63. La decisione dell’Autorità segue la posizione espressa dalle autorità nazionali responsabili dell’esecuzione della normativa a tutela dei consumatori in *Common position of national authorities within the CPC Network concerning the protection of consumers on social networks*, 17 marzo 2017, che invitano a considerare attentamente la possibile vessatorietà di alcune clausole contenute nelle condizioni generali predisposte dai gestori dei *social networks*.

¹⁵ Su cui v., *ex multis*, P. Sirena, sub *Art. 1469-ter*, 2° comma, in, G. Alpa, S. Patti (a cura di), *Clausole vessatorie nei contratti dei consumatori*, in *Il codice civile. Commentario* fondato da P. Schlesinger e diretto da F.D. Busnelli, Milano, 2003, 855 ss.; A. Fici, sub *Art. 34*, in E. Navarretta, A. Orestano (a cura di), *Dei contratti in generale*, in *Commentario del codice civile* diretto da E. Gabrielli, IV, Torino, 2011, 828 ss.

¹⁶ In tal senso cfr. F. Bilotta, *Consenso e condizioni generali di contratto*, in V. Cuffaro, V. Ricciuto (a cura di), *Il trattamento dei dati personali*, Torino, 1999, II, 103-104.

acconsenta al trattamento dei propri dati, difficilmente consente di argomentare nel senso della vessatorietà *tout court* di tali previsioni. Questo non significa che le clausole in questione non possano, a seconda delle circostanze, considerarsi vessatorie¹⁷, ma il loro mero inserimento in condizioni generali di contratto non ne determina automaticamente la vessatorietà.

Sotto il profilo della tutela del mercato, dunque, la principale preoccupazione è, preso atto del nesso di corrispettività di fatto esistente tra servizio e consenso al trattamento, esplicitarlo e renderlo trasparente (con le conseguenze che ne derivano in tema di rimedi), senza invece ambire a delimitarne i confini di liceità. Prendere in considerazione gli interessi degli utenti sottesi al mercato dei dati personali significa quindi regolarne la forma e non la sostanza. In altre parole, gli strumenti di regolazione del mercato e di tutela dei consumatori non sembrano essere attrezzati, salvo forzature, a indicare se sia lecito scambiare sul mercato i dati personali, ma segnalano solamente come tale scambio debba essere condotto.

3. I dati personali come controprestazione

Per capire come è regolato in via “sostanziale” il mercato dei dati personali occorre avere riguardo non al diritto dei consumi, ma alle norme in materia di protezione di dati personali. In particolare, la norma a cui fare riferimento è quella che prevede che il consenso al trattamento dei dati sia manifestato “liberamente”. Tale requisito – previsto già dalla direttiva 95/46/CE (art. 2, lett. *b*) e dal previgente codice della privacy (art. 23, c. 3) e poi ripreso dal regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati personali) – di per sé ci dice poco in mancanza di più precise indicazioni di quali siano le circostanze che rendono non “libero” il consenso. L’interpretazione che di tale norma è stata data dalle autorità garanti e dallo stesso legislatore europeo, che nel regolamento fornisce ulteriori specificazioni, l’ha resa il punto di riferimento per la questione che ci interessa.

Del problema della validità delle operazioni di *tying* in Italia si è occupato innanzitut-

¹⁷ In proposito v., in giurisprudenza, App. Roma, 24 settembre 2002, in *Giur. it.*, I, 2003, 119 ss., che ritiene vessatoria *ex artt.* 1469-*bis* ss., c.c. la clausola in base alla quale il cliente acconsente, nei confronti della banca, «al trattamento dei dati relativi sia a tutti i rapporti di affidamento-finanziamento, nonché eventuali carte di credito» e «a che tali dati accedano. [...] in genere i soggetti economici che ne facessero richiesta», osservando che tale clausola «costituisce un obbligo di “*pat?*” a carico del cliente, assai penetrante; imponendogli di consentire alla divulgazione, oltre che al trattamento, dei dati concernenti il rapporto contrattuale corrente con la banca, tutto ciò, senza che vi sia alcun vantaggio compensativo a sacrificio del diritto alla riservatezza, ottenuto in via preventiva ed irrevocabile (art. 20, 1° comma, lett. a), l. 31 dicembre 1996, n. 675); in questo modo realizzandosi uno squilibrio significativo in danno del consumatore»; Trib. Roma, 21 gennaio 2000, in *Foro it.*, I-2, 2000, 2045 ss., in cui si afferma che devono ritenersi abusive ai sensi degli artt. 1469 *bis* ss. c.c. le clausole che «obbligano il cliente a consentire in via preventiva il trattamento da parte della banca dei propri dati personali». In dottrina, cfr. C. Lo Surdo, *Commento ai provvedimenti adottati dall’autorità garante in merito al problema del consenso informato*, in *Danno e responsabilità*, 8, 1998, 645, la quale, con riferimento ai casi in cui il Garante «qualific[a] ogni forma di pressione esercitata sull’interessato al fine di carpirne il consenso come una “violazione della sua libertà contrattuale”», ritiene in proposito applicabile la disciplina sulle clausole vessatorie, per cui «il consenso non potrà infatti mai essere condizionato all’accettazione di clausole che determinino un significativo squilibrio dei diritti e degli obblighi delle parti ai sensi dell’art. 1469 *bis* c.c.».

to il Garante per la protezione dei dati personali, che l'ha risolto (in conformità con un'impostazione affermata in sede europea¹⁸) richiamandosi, per l'appunto, al requisito di libertà del consenso al trattamento. Pare dunque utile prendere le mosse da tali pronunce. Secondo un consolidato orientamento non è libero, ma "necessitato", il consenso a cui viene subordinato l'accesso a un bene o servizio: il consenso è dunque invalido e, conseguentemente, il trattamento illecito¹⁹. Ne deriva pertanto l'illiceità della prassi di subordinare l'accesso a un bene o servizio al consenso al trattamento dei dati personali per fini ulteriori rispetto a quanto necessario per fornire la prestazione. Se, come afferma il Garante, non è libero il consenso se posto come condizione per ricevere una controprestazione, pare porsi un ostacolo insormontabile alla possibilità di scambiare i dati personali sul mercato.

Tale utilizzo della nozione di libertà è peculiare. L'affermazione del Garante va ben al di là infatti di quanto comunemente inteso con "libertà del volere". "Consenso libero" è una formula vuota, che deve essere riempita dalle circostanze dequalificanti che si considerano rilevanti ai fini di invalidare l'atto. Nel diritto privato, esse sono rappresentate dall'incapacità, dai vizi del volere (errore, violenza, dolo) e, in casi particolari, dalla situazione di pericolo alla persona o di bisogno economico in cui si trova chi presta il consenso. Si tratta, come noto, dei casi di annullabilità e rescissione del contratto. L'impostazione di cui si discute attribuisce invece rilevanza a una circostanza che, negli atti di autonomia privata, è del tutto fisiologica: la necessità o il desiderio di procurarsi la controprestazione.

L'intento (o comunque il risultato) di tale approccio pare essere quello di scoraggiare lo sviluppo di un mercato basato sullo scambio di dati personali, limitando in tal modo i casi in cui i dati possono essere trattati. Come noto, vi sono diverse condizioni di liceità del trattamento; quella più sovente utilizzata dai soggetti privati è, tuttavia, il consenso dell'interessato, acquisito spesso anche in via cautelativa da chi tratta dati²⁰. Se per trattare i dati è normalmente richiesto il consenso ma si vieta di subordinare l'accesso a un servizio alla prestazione del consenso, è chiaro che raccogliere dati personali sarà più arduo, considerata anche l'incertezza che circonda alcune delle altre condizioni di

¹⁸ V. i riferimenti contenuti in S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Europa e diritto privato*, 2, 2016, 538-539, e in G. Resta, V. Zencovich, *op. cit.*, 429.

¹⁹ Tale affermazione, applicata in maniera pressoché costante dal Garante fin dai suoi primi anni di attività, è contenuta anche in un provvedimento a carattere generale: v. le *Linee Guida in materia di attività promozionale e contrasto allo spam*, in Registro dei provvedimenti 4 luglio 2013, n. 330. Per una ricognizione dei provvedimenti sul punto, sia consentito il rimando a S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, *cit.*, 532-538.

²⁰ L'ampio ricorso alla richiesta del consenso potrebbe in parte derivare dalla genericità con cui sono formulate altre condizioni di liceità del trattamento, tra cui, in particolare, quella del legittimo interesse. In altre parole, a fronte dell'incertezza in merito alla sussistenza di una condizione di liceità del trattamento, la prassi è quella di richiedere il consenso, anche in casi in cui probabilmente non ce ne sarebbe bisogno. La scelta di chiedere il consenso anche laddove ci sono altre condizioni che legittimano il trattamento non è però senza conseguenze: v. quanto affermato dal Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, 10 aprile 2018, 26, secondo cui una volta scelta una base legittima del trattamento non si può fare affidamento su una diversa base, con la conseguenza che, se si è chiesto il consenso e questo è revocato, occorre interrompere il trattamento. Per ulteriori considerazioni sia consentito il rimando a S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, *cit.*, 181.

liceità del trattamento. L'erogazione di beni e servizi è infatti l'occasione principale per raccogliere dati personali (come dimostrato dalla diffusione del *business model* di offrire servizi gratuitamente ma previo consenso al trattamento dei dati), ed è chiaro che impedire le operazioni di *tying* pregiudica la possibilità di raccolta. Se gli utenti devono essere liberi di accedere al servizio scegliendo se prestare o meno il consenso al trattamento dei dati, è infatti ben possibile che molti interessati decidano di negare il consenso, se ciò nonostante non viene loro impedito l'accesso al servizio.

Come accennato, questo modello di libertà del consenso si distanzia molto da quanto normalmente richiesto per tutelare la libertà del volere con riguardo agli atti di autonomia. Un simile modello presenta però qualche somiglianza con quanto previsto per gli atti di disposizione del corpo, rispetto a cui il nostro ordinamento vieta il collegamento sinallagmatico con una controprestazione e che proprio per questo vengono considerati come atti aventi contenuto non patrimoniale. Gli atti di disposizione del corpo, infatti, sono validi solo se posti in essere a titolo gratuito²¹. La gratuità dell'atto è volta a tutelare (non solo ma anche) la libertà del consenso del soggetto interessato²²; più precisamente, non si vuole che il volere sia inquinato da motivazioni economiche. In altre parole, almeno nel campo della biomedicina, l'integrità fisica non può essere scambiata con una prestazione e deve dunque rimanere fuori dei circuiti di mercato. Si può ritenere che questo sia il modello adottato anche con riguardo al "mercato" dei dati personali? Si può ritenere che il nostro ordinamento vieti lo scambio dei dati con una controprestazione (vieti, cioè, *tout court* di subordinare l'accesso a un bene o servizio alla prestazione del consenso al trattamento?)?

La risposta, contrariamente a quanto parrebbe emergere a prima vista dall'orientamento sopra descritto²³, non è costituita da un netto divieto, alla luce, in particolare,

²¹ Il principio di gratuità è affermato dalle singole leggi speciali che ammettono, in deroga a quanto previsto dall'art. 5 c.c., anche atti di disposizione del corpo che cagionino una diminuzione permanente dell'integrità fisica: si vedano, ad esempio, l'art. 6, l. 26 giugno 1967, n. 458 con riguardo alla donazione del rene; l'art. 1, d.lgs. 24 giugno 2003, n. 211 in materia di sperimentazione clinica; l'art. 4, l. 21 ottobre 2005, n. 219 in materia di donazione del sangue; l'art. 4, l. 6 marzo 2001, n. 52 con riguardo alla donazione di midollo. In via generale, il principio di gratuità si ritrova nelle fonti internazionali: l'art. 3 della Carta dei diritti fondamentali dell'Unione europea vieta di «fare del corpo umano e delle sue parti in quanto tali una fonte di lucro» e l'art. 12 della Convenzione di Oviedo dispone che «il corpo umano e le sue parti non debbono essere, in quanto tali, fonti di profitto». Sul tema v., per tutti, G. Resta, *Contratto e persona*, in V. Roppo, *Trattato del contratto*, IV, *Interferenze*, Milano, 2006, 17 ss.

²² Sul rapporto tra gratuità e libertà v., ad esempio, M.C. Venuti, *Atti di disposizione del corpo e principio di gratuità*, in A. Galasso, S. Mazzaresse (a cura di), *Il principio di gratuità*, Milano, 2008, 307-308. Si tenga però presente che in ambito di atti di disposizione del corpo la gratuità è posta anche a tutela di esigenze di solidarietà.

²³ Una posizione di netto sfavore verso la possibilità di scambiare i dati personali con un bene o servizio è tuttavia sostenuta dallo stesso Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, cit., 9, il quale, richiamandosi al considerando 43 del regolamento 2016/679, afferma che «[l']obbligo di acconsentire all'uso di dati personali aggiuntivi rispetto a quelli strettamente necessari limita la scelta dell'interessato e ostacola l'espressione del libero consenso. Poiché la legislazione in materia di protezione dei dati mira a tutelare i diritti fondamentali, è essenziale che l'interessato abbia il controllo sui propri dati personali; inoltre sussiste una presunzione forte secondo cui il consenso a un trattamento di dati personali non necessario non può essere considerato un corrispettivo obbligatorio dell'esecuzione di un contratto o della prestazione di un servizio». In questo senso v. J.P. Albrecht, *The EU's New Data Protection Law – How A Directive Evolved Into A Regulation*, in *Computer Law Review International*, 2, 2016, 36, il quale afferma categoricamente che «as a rule consent cannot be free if it is made a

di quanto previsto dal regolamento generale sulla protezione dei dati personali²⁴. In aggiunta a quanto previsto dalla previgente direttiva, il regolamento fornisce infatti ulteriori indicazioni in merito a che cosa debba intendersi per consenso “libero”, affermando che «[n]el 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» (art. 7, par. 4). Non è dunque vietato subordinare l’esecuzione di un contratto alla prestazione del consenso al trattamento dei dati, ma si tratta di una circostanza da tenere «nella massima considerazione» ai fini di valutare la libertà del consenso. Non pare dunque potersi trarre dalla norma un divieto generalizzato alle operazioni di *tying*; essa però non specifica in quali circostanze sia vietato subordinare l’accesso a un bene o servizio al consenso al trattamento.

È innanzitutto chiaro che una scelta libera manca qualora il consenso sia carpito con tecniche scorrette volte a coartare impropriamente la volontà dell’interessato. In questo modo si tutela l’integrità del volere in un’ottica non dissimile da quanto previsto in materia di pratiche commerciali scorrette. Una volta appurato che il consenso è stato prestato da un soggetto informato e in condizioni di serenità, ponderatezza e trasparenza, rimane il dubbio se i dati personali possano o meno essere oggetto di scambio. Allo stesso modo il consenso non è libero se prestato dall’interessato in una condizione di particolare vulnerabilità e debolezza, come nel caso di consenso al trattamento dei dati da parte del lavoratore nei confronti del datore di lavoro²⁵. Che cosa occorre affinché una scelta informata, serena, consapevole, ponderata e non viziata da una situazione di vulnerabilità sia anche “libera”?

Alcune indicazioni in proposito possono trarsi da quanto affermato dal Gruppo di lavoro Articolo 29, il quale ha precisato che la necessità che il consenso sia libero significa che «l’interessato abbia una scelta effettiva e il controllo sui propri dati»²⁶. Secondo questa interpretazione, l’effettività della scelta dipende dalla possibilità per l’interessato di accedere al servizio anche senza prestare il consenso al trattamento. Chi fornisce un servizio chiedendo il consenso al trattamento dovrebbe dunque offrire all’utente due versioni del servizio: l’una, condizionata alla prestazione del consenso, l’altra no. In una prima edizione delle nuove linee guida sul consenso, il Gruppo di lavoro aveva

condition for the execution of a contract despite not being necessary for that purpose».

²⁴ Nel senso che il regolamento non pone un divieto assoluto alle operazioni di *tying*, v. S. Thobani, *I requisiti del consenso al trattamento dei dati personali*, Santarcangelo di Romagna, 2016, 55; A. Metzger, *Data as Counter-Performance: What Rights and Duties do Parties Have?*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8, 2017, 5; E. Lucchini Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e impresa*, 1, 2018, 113; G. Resta, V. Zeno-Zencovich, *op. cit.*, 432.

²⁵ Lo stesso regolamento, al considerando n. 43, esclude che il consenso possa rappresentare una valida condizione di liceità del trattamento qualora vi sia un «evidente squilibrio» tra l’interessato e il titolare del trattamento, come nel caso in cui il titolare del trattamento sia un’autorità pubblica. V. in proposito le indicazioni fornite dal Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, cit., 6-8, in cui si porta come ulteriore esempio di squilibrio di potere quello relativo al rapporto tra datore di lavoro e lavoratore.

²⁶ Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, cit., 6.

affermato che «entrambi i servizi [quello subordinato e quello non subordinato al consenso al trattamento] devono essere genuinamente equivalenti, incluso senza ulteriori costi»²⁷. Volendo seguire fino in fondo tale indicazione, ne deriva che se la versione del servizio per cui si richiede il consenso al trattamento è offerta gratuitamente, altrettanto gratuita dovrebbe essere quella per cui non si richiede il consenso. Questa impostazione pare dunque precludere una qualunque possibilità di scambio dei dati personali con un bene o servizio.

In un secondo momento il Gruppo di lavoro ha però ammorbidito la propria posizione, limitandosi a richiedere che «i due servizi [debbano] essere effettivamente equivalenti»²⁸. Non è dunque più espressamente escluso che a rendere lecite le operazioni di *tying* sia la possibilità di accedere allo stesso servizio senza acconsentire al trattamento ma pagando una somma di denaro purché, chiaramente, si tratti di un corrispettivo congruo²⁹. L'effettività della scelta è garantita in questo modo dalla presenza di un'alternativa (non identica ma) equivalente.

Ci si può chiedere se un'alternativa equivalente possa ritenersi sussistente anche nel caso in cui un servizio analogo, per l'accesso al quale non sia richiesto il consenso al trattamento, venga offerto da un altro operatore sul mercato. È il caso, ad esempio, in cui sul mercato vi siano sia servizi di posta elettronica a pagamento per il cui utilizzo non è richiesto il consenso al trattamento ma un corrispettivo in denaro, sia servizi di posta elettronica “gratuiti” per cui viene invece richiesto il consenso all'utilizzo dei dati, offerti non dal medesimo ma da diversi operatori. Si deve trattare, chiaramente, di servizi effettivamente equivalenti; questo è da escludersi nel caso di servizi offerti da operatori sostanzialmente monopolistici³⁰: così, ad esempio, è difficile che, ad oggi, possa esservi un servizio di social network realmente equivalente a Facebook, o un motore di ricerca effettivamente equivalente a Google.

Il Gruppo di lavoro Articolo 29 esclude, tuttavia, che, qualora sul mercato siano presen-

²⁷ Article 29 Working party, *Guidelines on Consent under Regulation 2016/679*, 20 novembre 2017, 10.

²⁸ Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, cit., 10.

²⁹ Lo stesso Gruppo di lavoro aveva in precedenza aperto a tale possibilità: v. Article 29 Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 9 aprile 2014, 47, il quale afferma che «[i]n the context where consumers signing up for 'free' online services actually 'pay for' these services by allowing the use of their personal data, it would also contribute towards a favourable assessment of the balance – or towards the finding that the consumer had a genuine freedom of choice, and therefore valid consent was provided under Article 7(a) – if the controller also offered an alternative version of its services, in which 'personal data' were not used for marketing purposes». V. anche la posizione espressa dal Garante Europeo per la Protezione dei Dati, *Opinion 5/2016 Preliminary. EDPS Opinion in the review of the ePrivacy Directive (2002/58/EC)*, 22 luglio 2016, 15-16, secondo cui il fornitore del servizio deve «(i) either provide a choice whether or not to provide consent to processing data not necessary for the provision of the service without any detriment, (ii) or at least, make available a paying service at a reasonable price (without behavioural advertising and collection of data) as an alternative to the services paid by users' personal informations».

³⁰ O, per meglio dire, di servizi che offrono agli utenti utilità che altri servizi dello stesso tipo non riescono a offrire. In tale prospettiva potrebbe in parte leggersi la decisione del Bundeskartellamt, 6 febbraio 2019, B6-22/16, che ha proibito, in quanto abuso di posizione dominante, a Facebook di condizionare l'accesso al servizio (di social network e di altri servizi, quali WhatsApp e Instagram forniti dalla medesima società) al consenso al trattamento dei dati e di trattare tali dati congiuntamente alle informazioni generati dall'utente durante la navigazione su altri siti e raccolti senza il consenso degli interessati. Su tale caso, v. A. Palmieri, R. Pardolesi, *Abuso di posizione dominante e condizioni generali di contratto: un "revival innovativo"*, in *Foro italiano*, 3, 2018, 144 ss.

ti alternative offerte da operatori diversi, il consenso possa ritenersi libero, affermando che «[i]n tal caso la libertà di scelta dipenderebbe dagli altri operatori del mercato e dal fatto che l'interessato ritenga che i servizi offerti dall'altro titolare del trattamento siano effettivamente equivalenti» e che «[c]iò implicherebbe inoltre l'obbligo per il titolare del trattamento di monitorare gli sviluppi del mercato per garantire la continuità della validità del consenso [...] in quanto un concorrente potrebbe modificare il suo servizio in un momento successivo»³¹. Tali argomentazioni non paiono tuttavia decisive. Da un lato, la validità del consenso va valutata nel momento in cui esso è prestato, parendo irrilevante il successivo mutamento di circostanze. Si consideri che, potendo l'interessato liberamente revocare il consenso in qualunque momento, ben potrebbe l'utente revocare il consenso recedendo dal servizio e, verificato che sul mercato non ci sono più servizi equivalenti, pretendere di accedere nuovamente al servizio senza, questa volta, acconsentire al trattamento dei propri dati. Dall'altro, la difficoltà nel valutare la sussistenza dell'"equivalenza" si supera se, contrariamente a quanto pare adombrare il Gruppo di lavoro, se ne adotta una nozione oggettiva, legata alle caratteristiche del servizio e non, invece, alle idiosincrasie dei singoli interessati. Una diversa soluzione, che apra a una interpretazione fortemente soggettiva dell'equivalenza pare stonare rispetto a rapporti, come quelli in questione, solitamente di massa e del tutto spersonalizzati. "Consenso libero" significa dunque consenso prestato a fronte di un'"alternativa", che questa sia fornita dal medesimo o da diversi operatori. Tale soluzione è condivisa nel nostro ordinamento interno dalla Suprema Corte che, nell'unica pronuncia sinora sul punto, ha affermato che è lecito subordinare l'accesso a un bene o servizio alla prestazione del consenso al trattamento purché si tratti di un bene o servizio "fungibile"³². La fungibilità è intesa qui in senso atecnico proprio per indicare la possibilità di accedere a servizi analoghi³³ ed esprime dunque la necessità che vi sia, per l'appunto, un'alternativa. Il caso riguardava un servizio di *newsletter* su tematiche in materia di finanza, fisco, diritto e lavoro, informazioni che la Corte sottolinea essere «agevolmente acquisibili per altra via, eventualmente attraverso siti a pagamento, se non attraverso il ricorso all'editoria cartacea, con la conseguenza che ben può rinunciarsi a detto servizio senza gravoso sacrificio». A detta della Corte, le operazioni di *tying* sono dunque vietate se la prestazione è «ad un tempo infungibile ed irrinunciabile per l'interessato». Si introduce così un ulteriore elemento, quello della "irrinunciabilità", che si aggiunge all'infungibilità e che riguarda l'importanza della prestazione per l'utente³⁴.

³¹ Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, cit., 10-11.

³² Cass. civ., sez. I, 2 luglio 2018, n. 17278, in *Giur. it.*, 3, 2019, 530 ss.

³³ Si era proposto di utilizzare a tal fine il criterio della infungibilità così inteso in S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, cit., 547. Nello stesso senso si sono espressi G. Resta, V. Zeno-Zencovich, *op. cit.*, 432.

³⁴ Sull'importanza del fattore dell'essenzialità del servizio cfr. C. Lo Surdo, *Il ruolo dell'obbligo di informativa*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, I, 736; A. Orestano, *La circolazione dei dati personali*, *ivi*, 172. In proposito è interessante rilevare le modifiche intervenute da un'edizione all'altra del *Manuale sul diritto europeo in materia di protezione dei dati* redatto dall'Agenzia dell'Unione europea per i diritti fondamentali e dal Consiglio d'Europa: mentre nell'edizione del 2014 si affermava che «quando prodotti o servizi sufficientemente importanti possono essere ottenuti solo ed esclusivamente se alcuni dati personali sono comunicati a terzi, il consenso dell'interessato alla divulgazione dei propri dati di solito non può essere considerato frutto di una decisione libera» (61),

Sicuramente se il servizio è sia “infungibile” che “irrinunciabile”, cioè se si tratta di un servizio essenziale per l’interessato e di cui non vi è un equivalente facilmente accessibile, non sarà lecito condizionarne l’erogazione al consenso al trattamento dei dati. Si noti che, se una prestazione è fungibile, essa è in quanto tale anche rinunciabile, in quanto chi voglia usufruire di quel tipo di servizio ne ha comunque la possibilità. Questo non significa tuttavia che tutte le volte in cui un servizio sia fungibile sia possibile condizionarne l’accesso al consenso al trattamento dei dati, in quanto possono esservi altre circostanze che inquinano la libertà del consenso, come, ad esempio, una situazione di particolare debolezza e vulnerabilità dell’interessato. Così, ad esempio, un datore di lavoro o una struttura sanitaria non potrebbero chiaramente subordinare un’offerta di lavoro o l’erogazione delle cure al consenso al trattamento dei dati del lavoratore o del paziente, e questo anche qualora la prestazione sia fungibile (nel senso che vi sono altri datori di lavoro o altre strutture sanitarie che non richiedono il consenso all’utilizzo dei dati).

Problemi possono invece sorgere nel caso in cui il servizio sia infungibile ma non “irrinunciabile”. Si pensi al caso di Facebook: come si è detto prima, ad oggi Facebook è probabilmente un servizio infungibile, meno certo è se sia anche irrinunciabile ed essenziale. Sembra preferibile, in ogni caso, riservare la qualifica di rinunciabilità solo ai casi di più evidente futilità e al di fuori di questi ritenere che qualunque servizio che sia realmente infungibile – che, cioè, non presenti equivalenti sul mercato – sia anche irrinunciabile.

Questi, dunque, paiono essere i limiti entro cui è possibile richiedere i dati personali come controprestazione per un bene o servizio. Lo sviluppo di un mercato dei dati personali è dunque ammesso purché l’interessato abbia la possibilità di non entrarvi, dovendo egli avere, nel senso sopra precisato, un’“alternativa”. I modi in cui questa alternativa deve essere offerta sono disciplinati dalle norme in materia di tutela dei consumatori, che prescrivono che l’utente debba poter scegliere in maniera consapevole, informata, serena e ponderata. Tocca invece alle norme in materia di protezione dei dati personali stabilire quando tale alternativa è da considerarsi effettivamente sussistente.

nella successiva edizione del 2018 il riferimento alle circostanze che escludono la libertà del consenso è al caso in cui «prodotti o servizi possono essere ottenuti solo se alcuni dati personali sono comunicati al titolare del trattamento o successivamente a terzi» senza più alcuna menzione dell’importanza del prodotto o servizio in questione (162); d’altronde, anche nella seconda edizione rimane come esempio di valida operazione di *tying* quello di chiedere il consenso al trattamento per il rilascio di carte fedeltà, purché, tuttavia, l’operazione sia finalizzata a ottenere una «piccola riduzione del prezzo di determinati prodotti» (mentre, si noti, la prima edizione faceva riferimento a «riduzioni dei prezzi di determinati prodotti»). Il requisito della irrinunciabilità o essenzialità della prestazione offerta in cambio del consenso al trattamento parrebbe in parte assorbire un altro criterio che, come già accennato nel testo, dovrebbe essere tenuto in considerazione nel valutare se il consenso sia stato liberamente prestato, quello della disparità di potere tra le parti, nel senso che la disparità di una parte rispetto all’altra andrà valutata anche in considerazione dell’essenzialità, per la parte debole, del servizio fornito. Nello stesso senso si è espresso il Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, cit., 6-8, che, come si è accennato sopra, porta come esempio di casi in cui sussiste una disparità tale da compromettere la libertà del consenso le richieste di consenso al trattamento dei dati provenienti da autorità pubbliche o da datori di lavoro.

4. Profili di tutela dell'interessato

Occorre ora interrogarsi su quali siano le ragioni alla base dell'impostazione sin qui analizzata e quali, in particolare, gli interessi tutelati nel limitare come sopra descritto lo sviluppo del mercato dei dati personali.

Le limitazioni alla commerciabilità dei dati derivano, come si è visto, dalle norme in materia di protezione di dati personali e, in particolare, dalla norma che detta i requisiti di validità del consenso al trattamento, che deve essere "libero". Come noto, la normativa in questione contempera due contrapposti interessi: quello alla libera circolazione dei dati (nell'ottica dello sviluppo di un mercato unico dei dati), da un lato, e quello alla protezione dei dati personali, annoverato, quest'ultimo, tra i diritti fondamentali espressamente riconosciuti dall'UE, dall'altro³⁵.

Si deve tuttavia sottolineare che il c.d. diritto alla protezione dei dati personali non ha un contenuto omogeneo ed è anzi volto in via strumentale a tutelare interessi eterogenei, che vanno oltre quelli dei singoli interessati di volta in volta coinvolti. Sono note le origini della normativa in questione. Essa nasce per affrontare i rischi posti dal trattamento in massa dei dati, così come reso possibile dall'evoluzione tecnologica, non solo nei confronti del singolo individuo ma, soprattutto, nei riguardi della collettività: conformazione sociale, segregazione ed esclusione delle minoranze, discriminazione, controllo sociale e sorveglianza³⁶. In questo senso, il diritto alla protezione dei dati personali si differenzia nettamente dagli altri diritti della personalità, quali il diritto alla riservatezza e il diritto alla identità personale, che sono invece volti alla tutela di interessi, omogenei per ogni singolo diritto, riferiti al singolo (la sfera di intimità privata e la corretta rappresentazione della persona all'esterno).

Due notazioni sono necessarie. Innanzitutto, occorre sottolineare come il diritto alla protezione dei dati personali non rappresenti in sé un bene finale da tutelare, ma sia strumentale alla tutela di altri interessi³⁷. In secondo luogo, bisogna essere consapevoli che tali interessi non sono solo di natura individuale, ma riguardano anche la collettività.

Con riguardo a quest'ultimo profilo, non si intende dire che il diritto alla protezione dei dati personali non tuteli anche interessi individuali, ma che è fortemente presente l'esigenza di tutela di interessi collettivi³⁸, come dimostrato peraltro dal campo di ap-

³⁵ Art. 8, Carta dei diritti fondamentali dell'Unione Europea, rubricato «Protezione dei dati di carattere personale».

³⁶ Sull'evoluzione della disciplina in materia di protezione di dati personali, v. la ricostruzione svolta da A. Mantelero, *The future of consumer protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics*, in *Computer Law & Security Review*, 30, 2014, 647 ss. Tra coloro che, nel dibattito italiano, hanno sottolineato tali rischi v. S. Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica di diritto privato*, 4, 1997, 585 ss.; G. Mirabelli, *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *Diritto dell'informazione e dell'informatica*, 2, 1993, 314 ss.; A. Mantelero, *Attività d'impresa in Internet e tutela della persona*, Padova, 2004, 103 ss.; S. Niger, *Note sul diritto alla protezione dei dati personali*, in *Cyberspazio e diritto*, 1, 2004, 49 ss.; S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006, 63 ss.

³⁷ In tal senso v. F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civili commentate*, 2017, 401-402.

³⁸ In proposito, v. A. Mantelero, *Personal data for decisional purposes in the age of analytics: From an individual*

plicazione materiale del regolamento generale sulla protezione dei dati, costituito dal «trattamento interamente o parzialmente automatizzato di dati personali e [dal] trattamento non automatizzato di dati personali contenuti in archivi o destinati a figurarvi» (art. 2, par. 1). Il fenomeno che il legislatore intende disciplinare, in continuità con le precedenti fonti europee in materia³⁹, è dunque principalmente il trattamento posto in essere con le nuove tecnologie, al fine, per l'appunto, di fronteggiare i rischi sopra menzionati.

In quest'ottica, la limitazione dello sviluppo di un mercato di dati personali pare essere in buona parte volta alla tutela di interessi collettivi. Al titolare del trattamento interessa poco chi sia la persona cui i dati si riferiscono considerata nella sua individualità, la quale è invece tenuta in conto unicamente come punto di riferimento di informazioni, la cui aggregazione è utile per lo svolgimento di attività ulteriori (come inviare pubblicità mirata, effettuare ricerche di mercato o analisi predittive) in cui l'individuo è preso in considerazione come parte di una massa. Peraltro, le ricadute dirette del singolo trattamento su ciascun interessato sono spesso di poco conto; a dimostrazione di ciò, le conseguenze più pregnanti in caso di consenso invalido e dunque di trattamento illecito si collocano sul piano delle sanzioni amministrative e penali. Lo scopo delle limitazioni poste al mercato dei dati personali pare dunque essere quello di evitare che grazie alla mole di informazioni raccolte si pongano in essere condotte pregiudizievoli per la società in generale. Si utilizza pertanto uno strumento di tutela individuale (circondando di cautele la prestazione del consenso al trattamento del singolo interessato e limitando la possibilità di subordinare l'accesso a un bene o servizio al consenso al trattamento) per proteggere in realtà interessi generali messi a rischio dai trattamenti di massa.

Della dimensione collettiva del fenomeno e della generalità degli interessi coinvolti è consapevole il legislatore europeo, che adotta infatti una strategia differenziata per tutelare gli interessi in gioco, senza limitarsi alle cautele di cui circonda il consenso individuale. Non solo, da un lato, restringe la possibilità di raccogliere i dati, ma, dall'altro, impone (anche laddove i dati siano raccolti lecitamente) di effettuare comunque una valutazione dei rischi derivanti dal trattamento e di individuare le misure atte a contenerli. La limitazione alla possibilità di subordinare l'accesso a un bene o servizio al consenso al trattamento si colloca, per l'appunto, nella prima di tali strategie (diretta a limitare la raccolta dei dati), accanto ad altri strumenti, quali il principio di finalità e di minimizzazione del trattamento.

perspective to a collective dimension of data protection, in *Computer Law & Security Review*, 32, 2016, 239 ss.

³⁹ Il regolamento si pone in linea di continuità con gli strumenti normativi che in materia lo hanno preceduto: la direttiva 96/45/CE, che restringeva anch'essa il proprio campo di applicazione al trattamento automatizzato dei dati e a quello, anche non automatizzato, dei dati contenuti in archivi; la convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale adottata a Strasburgo il 28 gennaio 1981 (ratificata dall'Italia con l. 21 febbraio 1989, n. 98), che è applicabile solo alle «elaborazioni automatizzate di dati a carattere personale».

5. Considerazioni conclusive

La doppia prospettiva qui analizzata, della tutela del mercato e della tutela del diritto alla protezione dei dati personali, fa emergere la natura ambivalente delle informazioni personali, considerate ora come bene di natura economica, ora come oggetto di un diritto fondamentale. Si tratta di un'ambivalenza presente nella stessa normativa in materia di protezione di dati personali, posta a presidio, come si è accennato, sia della libera circolazione dei dati, sia della tutela degli interessati⁴⁰.

È un'ambivalenza che può portare a esiti contraddittori. Da un lato la normativa in materia di protezione di dati personali limita la raccolta dei dati e la possibilità di subordinare l'accesso a un bene o servizio alla prestazione del consenso al trattamento. Dall'altro, invece, la normativa in tema di protezione dei consumatori tende a riconoscere nella misura più ampia possibile il nesso sinallagmatico instaurato tra servizi e dati personali al fine di tutelare la trasparenza delle operazioni di mercato. Tale contraddizione è stata rilevata dal Garante europeo per la protezione dei dati personali, che, nel parere espresso sulla proposta di direttiva in materia di fornitura di contenuto e servizi digitali, ha per l'appunto contestato la qualifica dei dati personali come controprestazione⁴¹. La soluzione di compromesso raggiunta nella versione finale del testo della direttiva evita l'utilizzo del termine controprestazione con riguardo ai dati personali, affermando anzi che i dati non possono essere «considerati una merce»⁴², e riafferma in ogni caso la prevalenza della normativa in materia di protezione dei dati personali⁴³. Tale soluzione pare in realtà essenzialmente nominalistica, in quanto, a prescindere dalla qualifica formale dei dati come controprestazione, il caso in cui un servizio viene erogato a fronte del consenso al trattamento resta parificato, a livello di disciplina, a quello in cui è previsto un corrispettivo in denaro.

Per mitigare la contraddittorietà occorre differenziare i diversi piani su cui si pongono le normative in questione. Come si è detto, mentre la disciplina sui dati regola in via sostanziale il mercato dei dati personali, stabilendo se e quando il loro scambio è ammesso, la disciplina a tutela dei consumatori regola le modalità di tale scambio, garantendone la trasparenza e accordando ai consumatori determinati rimedi, a prescindere dalla liceità dello scambio.

Non può ad ogni modo negarsi la sussistenza delle due diverse spinte che animano il legislatore europeo. Da un lato, quella di tutela del mercato: in questa prospettiva si intende certamente garantire la trasparenza delle operazioni che coinvolgono dati personali, ma in definitiva se ne vuole anche agevolare la circolazione. Dall'altro, quella di tutela dei diritti fondamentali, rispetto a cui vi è la tendenza ad affermare un'area di

⁴⁰ Sul rapporto tra libertà economiche e il diritto alla protezione dei dati personali v. O. Pollicino [e M. Bassini], *Bridge is Down, Data Truck Can't Get Through... A Critical View of the Schrems Judgment in the Context of European Constitutionalism*, in G. Ziccardi Capaldo (a cura di), *The Global Community. Yearbook of International Law and Jurisprudence*, Oxford, 2016, 254, il quale sottolinea la dimensione assolutizzante che, perlomeno nella giurisprudenza della Corte di Giustizia, ha assunto il secondo rispetto alle prime.

⁴¹ Garante europeo per la protezione dei dati personali, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for supply of digital content*, cit.

⁴² Considerando 4.

⁴³ Considerando 37.

non-mercato quando sono in gioco valori indisponibili. I dati personali rientrano in questa area di non-mercato? Come si è tentato di argomentare, la risposta è negativa, anche se si tratta di un mercato strettamente regolamentato.

Come si è visto, ai fini di tale regolamentazione la scelta del nostro legislatore di fronte ai rischi posti dal trattamento dei dati personali è quella di reagire limitando la possibilità di trattare i dati stessi. A tale scopo, rispetto al consenso la strategia è quella di prevedere dei requisiti stringenti per la sua validità. Si tratta di un approccio (già ampiamente seguito dal legislatore europeo in sede di regolazione del mercato) che tenta di affrontare questioni che coinvolgono interessi superindividuali con strumenti di tutela dei singoli, che risultano così funzionalizzati a obiettivi esterni al singolo rapporto⁴⁴. Al di là dell'efficacia di tale soluzione (sono diffuse le perplessità sull'effettività del consenso quale strumento di tutela dei singoli)⁴⁵, pare ad ogni modo trattarsi di un approccio poco adeguato ad affrontare i rischi che la normativa in materia intende fronteggiare. Tali rischi si pongono infatti a valle del trattamento, risultando da ulteriori comportamenti posti in essere all'esito di esso. Si prenda ad esempio uno dei maggiori rischi posti dal trattamento in massa dei dati, quello di discriminazione. Intervenire a monte limitando la raccolta dei dati significa restringere la possibilità di differenziare le offerte di servizi anche in modalità non necessariamente discriminatorie (i fattori di discriminazione sono infatti tipici) e dunque non vietate nel nostro ordinamento. Affrontare i rischi a valle (liberalizzando, per così dire, la fase a monte) consentirebbe invece di aprire un dibattito per definire meglio (ed eventualmente ampliare) i risultati discriminatori vietati, dibattito che invece resta sullo sfondo se la soluzione adottata è quella di limitare *tout court* la raccolta dei dati.

L'impressione, in altre parole, è che non solo tale normativa riponga troppa fiducia, abusandone, nel consenso individuale, ma che sia essa stessa abusata nell'affrontare problemi che non necessariamente le appartengono.

⁴⁴ La letteratura sul punto è vastissima. V., da ultimo, A. Plaia, *Profili evolutivi della tutela contrattuale*, in *Europa e diritto privato*, 1, 2018, 69 ss.

⁴⁵ Sulla difficoltà di raggiungere soluzioni soddisfacenti attraverso una regolamentazione contrattuale del flusso dei dati personali, cfr. O. Ben-Shaha, L.J. Strahilevitz, *Contracting over Privacy: Introduction*, in *Journal of Legal Studies*, 45, 2016, S2-S5. Alla radice, come noto, vi sono i dubbi che investono la stessa opportunità di lasciare al consenso individuale le scelte in merito al trattamento dei dati: cfr., in tal senso, S. Rodotà, *Protezione dei dati e circolazione delle informazioni*, in *Rivista critica di diritto privato*, 4, 1984, 732-733; G. Mirabelli, *op. cit.*, 324; S. Simitis, *Il contesto giuridico e politico della tutela della privacy*, in *Rivista critica di diritto privato*, 1997, 567; C. Camardi, *Mercato delle informazioni e privacy – riflessioni generali sulla L. n. 675/1996*, in *Europa e diritto privato*, 4, 1998, 1061; V. Carbone, *Il consenso, anzi i consensi, nel trattamento informatico dei dati personali*, in *Danno e responsabilità*, 1, 1998, 30. Da un lato, infatti, numerosi studi hanno analizzato i limiti cognitivi degli utenti con riguardo alle scelte in materia di privacy: v., ad esempio, D.J. Solove, *Privacy Self-Management and the Consent Dilemma*, in *Harvard Law Review*, 126, 2013, 1883 ss.; L. Gatt, R. Montanari, I.A. Caggiano, *Consenso al trattamento dei dati personali e analisi giuridico comportamentale. Spunti di una riflessione sull'effettività della tutela dei dati personali*, in *Politica del diritto*, 2, 2017, 363 ss. Dall'altro, il consenso individuale potrebbe ad ogni modo non costituire lo strumento più adeguato laddove, come nel caso della raccolta in massa di dati personali, gli interessi coinvolti siano di carattere superindividuale: cfr., sul punto, le riflessioni svolte da A. Mantelero, *Personal data for decisional purposes in the age of analytics: From an individual perspective to a collective dimension of data protection*, *cit.*, 245 ss.