

IL CONSENSO NELLA REGOLAZIONE DELLA CIRCOLAZIONE DEI DATI

Di Shaira Thobani

| 469

SOMMARIO: 1. Il consenso come strumento di autodeterminazione. – 2. Il consenso come strumento per restringere l'uso dei dati. – 3. Il consenso come strumento per facilitare l'uso dei dati. – 4. I compiti impropri del consenso.

ABSTRACT. Il contributo analizza il ruolo del consenso individuale nell'uso dei dati, mettendo in dubbio che la perdurante previsione del consenso tra le basi legittimanti il trattamento dei dati personali sia volta a garantire una manifestazione di volontà attenta e consapevole, e proponendo invece di leggere il consenso come strumento finalizzato ad assicurare una circolazione dei dati coerente con le linee di politica del diritto che guidano il legislatore europeo nella costruzione di un'economia basata sui dati.

The article analyses the role of individual consent in data use, questioning whether the continuing requirement for consent as one of the bases for the legitimate processing of personal data is intended to guarantee a careful and informed expression of will. Instead, it proposes that consent should be seen as a tool aimed at ensuring data circulation consistent with the legal policy guidelines that guide the European legislator in building a data-based economy..



1. Il consenso come strumento di autodeterminazione.

Che nell'odierno mondo digitale il consenso al trattamento dei dati personali si è ormai ridotto a un feticcio volto ad ammantare di legittimità l'accumulo di informazioni da parte dei soggetti forti del mercato corrisponde quasi a un luogo comune¹. È certamente sotto agli occhi di tutti, e tutti ne facciamo quotidiana esperienza, che l'internauta medio non solo non legge le informative c.d. privacy (e, se le leggesse, probabilmente non le capirebbe), ma neppure si accorge di acconsentire al trattamento dei propri dati². Si potrebbe ipotizzare che negli ultimi anni si sia diffusa una certa generica consapevolezza nel largo pubblico in merito al fatto che coloro che offrono servizi online raccolgono dati e ne ricavano un qualche guadagno, ma le modalità con cui tale raccolta ed estrazione di valore in pratica avvengono rimangono, nella percezione comune, avvolte in una nube di incertezza. A fronte di questa situazione, la domanda che spontaneamente sorge è perché continuare a prevedere il consenso dell'interessato tra le basi legittimanti il trattamento dei dati personali.

Chi è perplesso sull'opportunità di lasciare all'interessato la decisione sulla circolazione dei propri dati lo è perché prende sul serio la nozione di consenso come atto di volontà intesa in senso soggettivo: se l'interessato non se ne accorge e non capisce, come si può sostenere che egli “voglia” acconsentire al trattamento? La risposta pare scontata: è chiaro che egli non

¹ Da tempo i giuristi manifestano perplessità sull'idoneità del consenso a consentire l'esercizio dell'autodeterminazione informativa da parte dell'interessato: v. ad es., S. RODOTÀ, *Protezione dei dati e circolazione delle informazioni*, in *Riv. crit. dir. priv.*, 1984, 732 s.; G. MIRABELLI, *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *Dir. inf.*, 1993, 324; S. SIMITIS, *Il contesto giuridico e politico della tutela della privacy*, in *Riv. crit. dir. priv.*, 1997, 567; C. CAMARDI, *Mercato delle informazioni e privacy – riflessioni generali sulla L. n. 675/1996*, in *Eur. dir. priv.*, 1998, 1061; V. CARBONE, *Il consenso, anzi i consensi, nel trattamento informatico dei dati personali*, cit., in *Danno resp.*, 1998, 30. La questione si è posta con ancora maggiore prepotenza all'attenzione degli interpreti a seguito dell'evoluzione tecnologica degli ultimi decenni: *ex multis*, D.J. SOLOVE, *Privacy Self-Management and the Consent Dilemma*, *Harv. L. Rev.*, 2013, 1880 ss.; L. GATT, R. MONTANARI, I.A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Pol. dir.*, 2017, 337 ss.; E. BIETTI, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, in *Pace Law Rev.*, 2020, 310 ss.; A. GAROFALO, *Regolare l'irregolabile: il consenso al trattamento dei dati nel GDPR*, in S. ORLANDO, G. CAPALDO (a cura di), *Annuario 2021 Osservatorio Giuridico sulla Innovazione Digitale*, Roma, 2021, 121 s.; A. GENTILI, *La volontà nel contesto digitale: interessi del mercato e diritti delle persone*, in *Riv. trim. dir. proc. civ.*, 2022, 703 ss.; I. COFONE, *The Privacy Fallacy. Harm and Power in the Information Economy*, Cambridge, Cambridge University Press, 2023, *passim*.

² Sulla incapacità degli interessati di adottare decisioni consapevoli con riguardo ai propri dati la letteratura è ormai estremamente vasta. V., *ex multis*, A. ACQUISTI, J. GROSSKLAGS, *Privacy and Rationality in individual Decision Making*, in *IEEE Security & Privacy*, 2005, 26 ss.; D.J. SOLOVE, *Privacy Self-Management*, cit., 1883 ss.; S. KOKOLAKIS, *Privacy Attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon*, in *Computers & Security*, 2017, 122 ss.; L. GATT, R. MONTANARI, I.A. CAGGIANO, *op. cit.*, 337 ss.; N. GERBER, P. GERBER, M. VOLKAMER, *Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior*, in *Computers & security*, 2018, 226 ss.



“vuole” in senso soggettivo-volontaristico. Se, oltre a ciò, consideriamo che l’interessato è solitamente chiamato a prestare il consenso in un ambiente digitale predisposto da chi ha interesse a raccogliere i dati e organizzato appositamente in modalità tali da agevolare la manifestazione del consenso³, allora difficilmente la volontà, anche laddove presente, potrebbe dirsi libera e genuina, in quanto spesso indotta da tecniche manipolatorie di vario tipo.

Che il consenso non sia necessariamente né sinonimo di volontà né baluardo di libertà è cosa ben nota al civilista⁴. Non tutti i fattori che perturbano la libertà sono infatti riconosciuti dal diritto come idonei a invalidare l’atto e, dove così non è, ben può capitare che il consenso, da strumento di libertà, si trasformi, di fatto, in strumento di oppressione⁵. L’avvento della società di massa ha reso ciò ancora più evidente: con il dilagare degli “scambi senza accordo” il ruolo della volontà del singolo si è gradualmente ridotto alla scelta della merce dallo scaffale⁶ e la tutela del contraente debole si è man mano spostata da un controllo sulla volontarietà e libertà dell’atto di consenso a un controllo sul contenuto del rapporto, volto ad assicurare che la parte forte non predisponga condizioni contrattuali (che l’altra parte probabilmente neppure conosce) eccessivamente sbilanciate a detrimento di quella debole. Se così è, non dovrebbe eccessivamente stupire che il consenso al trattamento dei dati personali spesso non sia né volontario, né libero. Occorre dunque innanzitutto chiedersi per quali profili il tema del consenso con riguardo ai dati diverga rispetto a fenomeni già ampiamente noti e studiati.

Di nuovo e di diverso rispetto agli scambi senza accordo dei mercati di massa è innanzitutto che, mentre il consumatore (che pure spesso non legge le condizioni contrattuali) è in grado di apprezzare il valore del denaro che presta come corrispettivo, nel caso delle richieste di consenso al trattamento dei dati personali l’interessato non ha normalmente la benché minima consapevolezza di che cosa significhi che i suoi dati siano trattati. In altre parole, mentre nei rapporti classici tra professionista e consumatore quest’ultimo è consapevole del valore del denaro che costituisce elemento essenziale della transazione, nei rapporti tra titolare e interessato quest’ultimo non è normalmente in grado di rendersi conto (non solo delle condizioni giuridiche dell’accordo ma neppure) che la controparte gli stia chiedendo qualcosa dotato di una qualche utilità⁷. Questo è in effetti il principale argomento utilizzato per mettere in serio dubbio l’opportunità di mantenere il consenso come base giuridica legittimante il trattamento, specie se lo scopo di tale pre-

³ Una descrizione accurata di tali modalità è contenuta nelle Linee guida 3/2022 del Comitato europeo per la protezione dei dati personali, *Modelli di progettazione ingannevoli nelle interfacce delle piattaforme di social media: come riconoscerli ed evitarli*, versione 2.0, 14.2.2023.

⁴ G. FINOCCHIARO, *Consenso al trattamento e libertà*, in *Persona mercato*, 2024, 10 s.

⁵ Cfr. M. FABRE-MAGNAN, *L’institution de la liberté*, PUF, Parigi, 2018, *passim*.

⁶ N. IRTI, *Scambi senza accordo*, in *Riv. trim. dir. proc. civ.*, 1998, 347 ss.

⁷ A. GAROFALO, *op. cit.*, 129 s. Questo deriva dal fatto che, nei trattamenti di massa, il valore dei dati è dato dalla massa dei dati (e non è invece dei dati singoli) e dalle operazioni che su di essi vengono compiute (operazioni che gli interessati non hanno la capacità di compiere): dunque, i singoli interessati non sono in effetti in grado di estrarre valore dai dati che li riguardano.

visione è quello di promuovere un controllo diffuso sui dati e garantire su di essi una sorveglianza effettiva da parte dell'interessato, che egli non è però in grado di compiere.

Tali dubbi sono frutto di una prospettiva che pone l'autodeterminazione informativa, e dunque il consenso dell'interessato, al centro della disciplina dell'uso e della circolazione dell'informazione. Nell'ordinamento europeo il diritto alla protezione dei dati personali si è infatti sviluppato in stretta connessione con il diritto all'autodeterminazione informativa⁸, il quale, collocando saldamente la protezione dei dati nell'ambito dei diritti fondamentali⁹, ha dato adito al diffondersi di una prospettiva che non solo considera il controllo da parte dell'interessato come il principale strumento di tutela dei dati personali, ma che, configurando questi ultimi come attributi immateriali della personalità, ritiene che sia la persona a dover decidere in merito alla loro circolazione. Si noti che si tratta di una impostazione che non corrisponde pienamente a quella adottata in sede legislativa: il diritto soggettivo dell'individuo è infatti “alla protezione dei dati di carattere personale che lo riguardano” (art. 8, par. 1, Carta dei diritti fondamentali dell'UE) e non “su” tali dati e ben potrebbe dunque esplicarsi in forme di controllo e protezione che non comportino necessariamente la legittimazione a prendere decisioni in merito all'utilizzo delle informazioni. Inoltre, il consenso è solo una delle basi legittimanti il trattamento, tra le quali figura anche il legittimo interesse di chiunque, diverso dall'interessato, intenda usare i dati¹⁰: l'interessato non ha dunque alcuna posizione di tipo proprietario sulle informazioni che lo riguardano¹¹. E tuttavia è forte l'impressione che tale prospettiva sia ancora ampiamente diffusa tra gli interpreti, che a lungo hanno considerato il consenso come la principale condizione di liceità del trattamento e che sembrano imputare alle deficienze della volontà degli interessati gran parte della

⁸ Cfr. I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale*, in *Annali dell'Università degli Studi Suor Orsola Benincasa*, 2016-2018, 12 e 31. Sugli equivoci e sulle incongruenze derivanti dalla costruzione del diritto alla protezione dei dati personali come diritto (fondamentale) dell'interessato all'autodeterminazione informativa, v. F. THOUVENIN, *Informational Self-Determination: A Convincing Rationale for Data Protection Law?*, in *JIPITEC*, 2021, 246 ss. Si tratta, a ben vedere, di un equivoco non lontano da quello segnalato da V. RICCIUTO, *L'equivoco della privacy. Persona vs dato personale*, Napoli, 2022, il quale denuncia la confusione tra il diritto alla riservatezza come tradizionalmente intesa e il diritto alla protezione dei dati personali.

⁹ Art. 8, Carta dei diritti fondamentali dell'UE. In senso critico verso la qualificazione del diritto alla protezione dei dati personali come diritto fondamentale, v. B. VAN DER SLOOT, *Legal Fundamentalism: Is Data Protection Really a Fundamental Right?*, in R. LEENES, R. VAN BRAKEL, S. GUTWIRTH, P. DE HERT (a cura di), *Data protection and Privacy: (In)visibilities and Infrastructures*, Springer, Cham, 2017, 3 ss.

¹⁰ Art. 6, par. 1, lett. f, Regolamento generale sulla protezione dei dati UE 2016/679 (GDPR). Anche l'art. 8, par. 2 della Carta dei diritti fondamentali dell'UE parla del consenso o di un “altro fondamento legittimo previsto dalla legge”.

¹¹ Ci si è interrogati sulla possibilità di configurare rispetto ai dati una disciplina di tipo proprietario. Sul tema cfr. P.M. SCHWARZ, *Property, Privacy and Personal Data*, in *Harvard Law Rev.*, 2004, 2055 ss.; N. PURTOVA, *Property Rights in Personal Data: A European Perspective*, Alphen aan den Rijn, 2011; C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, Torino, 2020, *passim*; S.H. HAZEL, *Personal Data as Property*, in *Syracuse L. Rev.*, 2020, 1055 ss.



responsabilità per l'attuale stato di circolazione incontrollata e senza freni delle informazioni¹².

In quest'ottica, tutti i tentativi di garantire la consapevolezza dell'interessato tramite la previsione di requisiti stringenti sembrano essere vani: le previsioni normative per cui il consenso deve essere non solo informato, ma anche specifico (e dunque non vale a legittimare trattamenti le cui finalità sono generiche o eterogenee), inequivocabile innanzitutto all'interessato (e quindi sono illegittimi i trattamenti a cui l'interessato acconsente senza rendersene conto) e libero (e dunque all'interessato deve essere data una alternativa realisticamente percorribile per non prestare il consenso) paiono molto lontane da quanto accade¹³. Qui risiede un altro elemento che caratterizza il problema del consenso al trattamento dei dati personali: la discrasia tra gli affanni degli interpreti, e in particolare delle autorità di controllo, volti faticosamente a circondare il consenso di cautele estreme come baluardo contro i rischi posti dal trattamento in massa dei dati, da un lato, e la facilità con cui in pratica il consenso è prestato e i dati sono accumulati, dall'altro.

Per capire come si è arrivati a questa situazione e sbrogliare quello che è stato definito come un “consent dilemma”¹⁴ – la difficoltà a fare a meno del consenso per il trattamento dei dati personali, da un lato, e a garantire che esso sia frutto di una volontà genuina, dall'altro, per cui nessuna delle soluzioni possibili (mantenere il consenso come condizione legittimante il trattamento oppure eliminarlo) soddisfa pienamente – può essere utile affiancare alla prospettiva soggettivo-individuale, che vede il consenso esclusivamente come atto di autonomia dell'interessato, una oggettiva e di mercato, che inserisce il consenso nel contesto più allargato della governance dei dati, in cui la questione principale è quella di decidere come e da parte di chi le informazioni possano essere utilizzate. La disciplina in materia di dati personali regola infatti la circolazione e l'utilizzo delle informazioni di carattere personale: a fronte dell'evoluzione tecnologica e sociale, il legislatore europeo si è assunto il compito, immane, di disciplinare un'utilità quale le informazioni (personali) di valore estremamente variabile, di difficile appropriabilità e controllo e di carattere estremamente eterogeneo con riguardo agli interessi coinvolti, tentando di trovare un difficile equilibrio tra questi ultimi. L'interrogativo di fondo riguarda dunque la misura in cui facilitare o restringere la circolazione e l'uso delle informazioni. Le soluzioni sono varie e spaziano da una circolazione pienamente libera – in cui chiunque può

¹² Si noti, tuttavia, che la previsione del consenso dell'interessato come base legittimante il trattamento non può considerarsi la sola (e neppure la principale) causa della circolazione incontrollata dei dati e dell'accumulo di masse di dati. Essa è semplicemente quella che a lungo è stata percepita come la più sicura entro cui trincerarsi per giustificare la liceità del trattamento, con argomentazioni che sono tuttavia puntualmente smentite dalle autorità di controllo quando hanno modo di scrutinare le operazioni di trattamento. Il problema è piuttosto che è estremamente difficile sottoporre a efficace controllo la circolazione di un bene immateriale quale l'informazione.

¹³ Su tali requisiti, v. EDPB, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, versione 1.1, 4.5.2020.

¹⁴ D.J. SOLOVE, *Privacy Self-Management*, cit., 1894.

trattare qualunque informazione per qualsivoglia finalità¹⁵ – a una pienamente controllata – in cui i dati possono essere utilizzati solo nei casi e per gli scopi previsti dal legislatore. La disciplina in materia di dati personali, e le previsioni sul consenso ivi contenute, non possono leggersi senza prendere in considerazione questi obiettivi e senza verificare come il consenso si collochi nel contesto di una tale strategia. Come vedremo, in quest’ottica un consenso facile da ottenere non pone particolari problemi se lo scopo è quello di incentivare la circolazione delle informazioni; al contrario, un consenso circondato da requisiti stringenti, che è dunque molto difficile da raccogliere validamente, si inserisce coerentemente in un quadro in cui l’obiettivo è quello di restringere l’uso dei dati.

Si è detto “affiancare” e non “sostituire” l’una prospettiva con l’altra. Vi sono infatti alcuni casi in cui il consenso dell’interessato rileva principalmente come espressione dell’autodeterminazione del soggetto. Questo si verifica quando il trattamento ha un impatto diretto e immediato sull’interessato, il quale è in grado di percepire chiaramente le conseguenze del trattamento in quanto esse si producono direttamente nella sua sfera¹⁶. Chi, se non la persona ritratta, dovrebbe decidere in merito alla pubblicazione della propria immagine (in assenza, chiaramente, di un interesse pubblico)? Chi, se non l’interessato, dovrebbe decidere se ricevere telefonate promozionali? Chi, se non il lavoratore, dovrebbe decidere se condividere informazioni di carattere privato con il proprio datore? Vi sono invece altri casi in cui il trattamento ha un impatto solo indiretto ed eventuale sui singoli interessati, mentre le conseguenze più rilevanti si producono nei confronti di terzi o della collettività (si pensi, ad esempio, ai rischi di segregazione delle minoranze, di indebita influenza dell’opinione pubblica, di conformazione sociale ecc.)¹⁷. In tali ipotesi non è centrale l’esigenza di tutelare l’autodeterminazione del singolo e l’opportunità di prevedere il consenso come base legittimante il trattamento risulta problematica. Innanzitutto perché, laddove il trattamento non abbia un qualche impatto immediatamente percepibile da parte dell’interessato, egli difficilmente presterà attenzione e

¹⁵ Si tratta del modello auspicato dall’analisi economica liberista: R.A. POSNER, *The Right of Privacy*, in *Georgia Law Rev.*, 1977, 393 ss.

¹⁶ La questione può leggersi come collegata a quella relativa al risarcimento del danno per trattamento illecito dei dati, in cui la verifica in merito all’ingiustizia del danno si traduce nella ricerca di un interesse leso che sia un interesse del singolo. Sul tema sia consentito il rimando a S. THOBANI, *Il danno non patrimoniale da trattamento illecito dei dati personali*, in *Dir. inf.*, 2017, 428 ss. e ai riferimenti ivi contenuti. Interessante in proposito è la recente evoluzione della giurisprudenza europea, che, in un’ottica di effettività delle tutele, tende ad ampliare la possibilità di ottenere un risarcimento: in tema cfr., di recente, C. CAMARDI, *Illecito trattamento dei dati e danno non patrimoniale. Verso una dogmatica europea*, in *Nuova giur. civ. comm.*, 2023, 1136 ss.; C. SCOGNAMIGLIO, *Danno e risarcimento nel sistema del RGPD: un primo nucleo di disciplina eurounitaria*, ivi, 1150 ss.; G. Buset, *Ingiustizia del danno e anti-giuridicità del fatto nella responsabilità da trattamento di dati personali*, in *Riv. dir. civ.*, 2024, 1008 ss.

¹⁷ Sulla dimensione collettiva delle conseguenze del trattamento dei dati personali v., ad es., A. MANTELERO, *Personal data for decisional purposes in the age of analytics: From an individual perspective to a collective dimension of data protection*, in *Computer Law & Security Rev.*, 2016, 245 ss.; B. VAN DER SLOOT, *The Quality of Life: Protecting Non-Personal Interests and Non-Personal Data in the Age of Big Data*, in *European Rev. Priv. Law*, 2021, 764 s.

sarà in grado di prestare un consenso consapevole; in secondo luogo, perché l'interessato neppure appare il soggetto più adatto a prendere decisioni le cui conseguenze si producono sui terzi e sulla collettività. Questi sono i casi in cui più è evidente come la disciplina del consenso (laddove sia previsto tra le basi di legittimità del trattamento) sia strumentale non tanto a tutelare la volontà dell'interessato, quanto a facilitare o restringere il flusso delle informazioni.

La disciplina in materia di dati personali non distingue, tuttavia, il primo dal secondo caso e ha al contrario un campo di applicazione estremamente ampio e indifferenziato. Basta considerare le definizioni di “dato personale” (qualunque informazione riconducibile a una persona fisica identificata o identificabile) e di “trattamento” (qualunque operazione sui dati) per rendersi conto della eterogeneità delle fattispecie che vi rientrano¹⁸: dalla profilazione per finalità di marketing, alla pubblicazione dell'immagine di un attore; dall'uso dell'indirizzo email per l'invio di comunicazioni commerciali, all'analisi dei dati relativi alla salute per finalità di trattamento sanitario; dall'esame delle informazioni sui sinistri dell'assicurato per fissare il suo livello di rischio, all'uso delle informazioni sugli incidenti di una certa zona per fissare i premi assicurativi di coloro che sono ivi residenti. Accomunando sotto un'unica regolamentazione un ventaglio di ipotesi estremamente variegata, di cui alcune difficilmente possono prescindere dalla necessità del consenso dell'interessato, la normativa in questione non può che continuare ad annoverarlo tra le basi legittimanti il trattamento.

Sarebbe senz'altro utile un'opera di perimetrazione, che restringa il campo di applicazione della disciplina in questione¹⁹, o che per lo meno effettui un'attenta distinzione tra le fattispecie, mantenendo il consenso come condizione di liceità del trattamento solo nei casi in cui vi siano conseguenze dirette e immediatamente percepibili dal singolo (e chiarendo se negli altri casi le informazioni possano essere utilizzate liberamente o solo nelle eventualità e per le finalità previste dal legislatore). Tale soluzione, per non dare luogo a fattispecie dai contorni fumosi fonte di forte incertezza, richiederebbe tuttavia una delimitazione piuttosto stringente e precisa, che il legislatore europeo è tendenzialmente restio a fare in settori (come quello di specie) a rapida evoluzione tecnologica. Questo fa sì che dal consenso sia difficile sfuggire sino a quando il campo di applicazione della normativa in materia di dati personali rimarrà così ampio e indistinto e che esso possa applicarsi, sotto un'unica etichetta, a casi in cui gli interessi in gioco sono molto diversi.

¹⁸ V. N. PURTOVA, *The Law of Everything. Broad Concept of Personal Data and the Future of EU Data Protection Law*, in *Innovation & Tech*, 2018, 40 ss.

¹⁹ Questo era il senso di S. THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Europa dir. priv.*, 2016, 513 ss. Per una rilettura della nozione di dato personale atta a limitare il campo di applicazione del GDPR ai soli casi in cui può ravvisarsi un interesse del singolo a controllare la circolazione delle informazioni, v. M.L. MONTAGNANI, M. VERSTRAETE, *What Makes Data Personal?*, in *UC Davis L. Rev.*, 2023, 1165 ss.

2. Il consenso come strumento per restringere l'uso dei dati

Proviamo ora ad analizzare in che modo, al di fuori dei casi in cui vi sono effettive esigenze di tutela dell'autodeterminazione informativa dei singoli, il consenso possa meglio leggersi come strumento che regola i flussi di informazione a prescindere dalla volontà dell'interessato e seguendo piuttosto obiettivi di politica del diritto.

Se la questione regolatoria principale è quella di restringere o facilitare l'utilizzo delle informazioni, la strada più piana su cui intervenire è quella delle basi legittimanti il trattamento: così, se lo scopo è quello di allargare il flusso dei dati, lo strumento più adatto è quello di liberalizzarne la circolazione; se invece l'obiettivo è quello restringerlo, si prevederanno basi di legittimità più specifiche (ammettendo solo i trattamenti condotti per determinate finalità stabilite dal legislatore). Il legislatore europeo ha adottato una via intermedia, disponendo che le informazioni possano essere liberamente utilizzate in presenza di un "legittimo interesse" del titolare del trattamento e riservando il consenso dell'interessato ai casi in cui questo interesse manchi.

Tale equilibrio tra le diverse condizioni di liceità del trattamento (che, si ribadisce, è centrale nell'individuare il punto di bilanciamento tra le diverse esigenze di maggiore o minore uso delle informazioni) è stato tuttavia del tutto distorto dalla prassi di chiedere sempre il consenso dell'interessato. È infatti noto come gli interventi legislativi europei abbiano portato a un'esplosione delle richieste di consenso al trattamento, il quale nella fase iniziale di applicazione della nuova normativa era evidentemente ritenuto la base legittima più sicura. Senza il consenso dell'interessato, infatti, si sarebbe dovuta individuare un'altra condizione legittimante il trattamento, individuazione non facile stante l'incerta interpretazione delle singole fattispecie di cui all'art. 6 GDPR e, in particolare, del legittimo interesse. Il legislatore non ha fornito ulteriori indicazioni su che cosa debba con esso intendersi, né si tratta di una clausola generale di per sé immediatamente decifrabile: questo ha inevitabilmente condotto a una forte incertezza e, conseguentemente, a una diffidenza da parte di chi tratta i dati ad appoggiarsi su tale base. I dubbi sulla sussistenza o meno di un legittimo interesse (che escluderebbe la necessità di chiedere il consenso dell'interessato), unitamente al principio di *accountability* (per cui sta al titolare, in assenza di indicazioni normative specifiche, decidere come declinare i principi generali dettati dal legislatore in ciascun singolo trattamento che pone in essere) e alla facilità, in pratica, di raccogliere il consenso (a fronte di interessati che sono molto facilmente indotti a cliccare "Sì acconsento") ha pertanto portato i titolari a preferire il consenso come base legittimante.

In un contesto, dunque, dove le altre basi legittimanti sono state a lungo guardate con sospetto e poco sviluppate nelle loro potenzialità, il consenso ha iniziato a essere chiamato in causa per giustificare trattamenti rispetto ai quali esso risulta però del tutto inadeguato: il riferimento è, come si è accennato, a tutti quei casi in cui manca un impatto diretto e percepibile sull'interessato, il quale dunque difficilmente sarà in grado di esprimere una



volontà consapevole e genuina²⁰. In tal modo il consenso ha assunto una centralità che non necessariamente avrebbe dovuto rivestire, incanalando gli sforzi degli interpreti (e in particolare delle autorità di controllo che, a fronte di trattamenti basati impropriamente sul consenso, spesso si trovano a dover valutare non la sussistenza di un legittimo interesse a trattare i dati ma la validità di consensi inconsapevoli) verso la ricerca di garanzie per assicurare un consenso genuino in circostanze in cui tale ricerca è poco utile. L'impressione è che le letture date al consenso e ai suoi requisiti, interpretati in maniera piuttosto restrittiva dai garanti, siano originate da un utilizzo improprio di tale base legittimante, che ha chiuso spazi a una riflessione più meditata sull'opportunità di ammettere o meno l'uso delle informazioni sulla base di altre condizioni di liceità.

Questo si è inserito in un contesto normativo, quello del GDPR, la cui principale preoccupazione è stata quella, a fronte della sempre maggiore raccolta e condivisione dei dati personali, di costruire un robusto sistema di protezione che, senza limitare la libera circolazione dei dati all'interno dell'UE, garantisse al contempo tutele adeguate²¹. In tale direzione vanno i principi generali del trattamento, improntati alla logica della minimizzazione e della limitazione delle finalità e, cioè, all'obbligo di trattare i dati il meno possibile e nei limiti strettamente necessari a raggiungere le finalità specificamente individuate. In questo senso gli interpreti hanno spesso individuato lo strumento di protezione più adatto nella restrizione, a monte, della circolazione dei dati, in un'ottica di precauzione.

Dunque, se lo scenario normativo è stato percepito (a ragione o a torto è difficile dire, data l'ambiguità di molte disposizioni del GDPR) come diretto a restringere l'uso delle informazioni e il canale principale attraverso cui le informazioni circolano è il consenso, allora non stupiscono le interpretazioni estremamente restrittive date dalle autorità di controllo sui suoi requisiti di validità. Esse vanno lette come tentativi non tanto di garantire manifestazioni di volontà genuine, ma di limitare la circolazione delle informazioni ragionando impropriamente sul consenso e non sulla sussistenza o meno di altre condizioni di liceità.

Questo emerge in maniera evidente laddove la prestazione del consenso rischia di facilitare eccessivamente la circolazione dei dati. Un caso sintomatico è quello della diffidenza che ha suscitato il diffondersi dei modelli c.d. *pay or consent*, in cui il prestatore di un servizio offre all'utente la scelta se pagare un corrispettivo in denaro oppure acconsentire al trattamento dei propri dati per finalità non necessarie all'esecuzione della prestazione (in particolare, per scopi di pubblicità comportamentale)²². Nonostante il legislatore non la vieti²³, il Comitato europeo per la protezione dei dati ha

²⁰ Questo è probabilmente il fenomeno alla base del c.d. paradosso della privacy.

²¹ V. i considerando nn. 6-7, GDPR.

²² Sulle questioni sollevate dal diffondersi di tali modelli v. E. Alonzo, *Pubblicità comportamentale online e schemi emergenti di negoziazione del consenso al trattamento dei dati personali. Il modello "pay or consent"*, in *Jus civile*, 2025, 134 ss.

²³ La questione è quella della commerciabilità dei dati personali su cui v., ad es., I.A. CAGGIANO, *op. cit.*, 23 ss.; S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018, 158 ss.; V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostru-*

espreso parere negativo in merito alla liceità di tale prassi con riguardo alle piattaforme online di grandi dimensioni, le quali dovrebbero tendenzialmente offrire anche la possibilità di accedere a versioni equivalenti dello stesso servizio senza trattare i dati e senza chiedere un corrispettivo in denaro²⁴.

A fronte di piattaforme dotate di una posizione dominante sul mercato, il timore esplicitamente manifestato dal Comitato è che gli interessati siano privati della possibilità di accedere a un servizio senza dover per forza, pur di non vedere trattati i propri dati, pagare un prezzo in denaro. Il problema di fondo non sembra però riguardare la genuinità del consenso individuale, nonostante le argomentazioni basate sul requisito della libertà e su un supposto divieto di commercializzazione, ma la eccessiva facilità della circolazione delle informazioni che può derivare dalle scelte degli interessati. La decisione di non pagare un prezzo, benché minimo, ma di acconsentire al trattamento dei propri dati (specie laddove l'impatto di tale singolo trattamento si produca non tanto sull'interessato ma sulla collettività in generale) è lungi dall'essere una scelta inconsapevole e non genuina da parte del singolo e, anzi, potrebbe essere considerata frutto di un calcolo razionale da parte di utenti che normalmente non subiscono alcuna conseguenza particolarmente negativa direttamente collegata alla loro singola scelta²⁵. La possibilità di accedere a servizi senza pagare un prezzo in denaro è infatti estremamente appetibile e, mentre è irrealistico pensare che l'interessato medio abbia il tempo e le capacità di leggere tutte le informative privacy in cui si imbatte quotidianamente, non sarebbe così strano ipotizzare che lo stesso scelga deliberatamente, specie quando il trattamento non ha un impatto immediato e diretto su di esso, di preferire comunque (anche senza informar-

zione del fenomeno, in *Dir. inf.*, 2018, 689 ss.; G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, 411 ss.; 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. impr.*, 2019, 34 ss.; A. VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale*, Napoli, 2019, 99 ss.; G. D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Dir. inf.*, 2020, 634 ss.; R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contr. impr.*, 2020, 760 ss.; G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020; C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, *passim*; C. SOLINAS, *Autonomia privata e regolazione pubblica nel trattamento dei dati personali*, Bari, 2022, 53 ss.; V. BACHELET, *Il consenso oltre il consenso. Dati personali, contratto, mercato*, Pisa, 2023, 76 ss.; C. MIGNONE, «Giornata perfetta». *La patrimonializzazione dei dati personali tra inconvenienti della retorica ed esigenze della pratica*, in *Persona mercato*, 2024, 49 ss.

²⁴ EDPB, *Parere 8/2024 sul consenso valido nel contesto dei modelli "consenso o pagamento" attuati dalle piattaforme online di grandi dimensioni*, 17.4.2024.

²⁵ Sottolinea come le previsioni del GDPR sui requisiti del consenso sono basate su una concezione meramente individualista della protezione dei dati personali, che non tiene conto delle externalità negative del trattamento, Y. HERMSTRÜWER, *Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data*, in *JIPITEC*, 2017, 9 ss. Questo vale, a maggior ragione, in un sistema come quello europeo in cui, in ogni caso e a prescindere dal consenso (come si dirà poco più avanti nel testo), sono vietati i trattamenti più rischiosi con un impatto negativo sui diritti e le libertà dei singoli, i quali possono dunque dormire sonni relativamente tranquilli vista la vigilanza comunque effettuata della autorità di controllo e la protezione innanzi ad esse comunque invocabile.

si²⁶) il trattamento dei suoi dati rispetto al pagamento di un corrispettivo monetario²⁷. Sicuramente gli interessati nella maggior parte dei casi non sono consapevoli degli effetti su larga scala che il cumulo dei consensi produce: ma sarebbe ben strano (o comunque lontano dalle logiche che operano nel diritto privato con riguardo agli atti di autonomia) affermare che una scelta individuale non è genuina solo perché non prende in considerazione il suo impatto sulla collettività.

Il problema dei modelli *pay or consent* – specie, per l'appunto, se adottati da chi ha sul mercato posizioni importanti – è allora quello di rendere fin troppo preferibile, nella prospettiva di un calcolo costi-benefici effettuato in una prospettiva meramente individuale, la scelta di acconsentire al trattamento dei dati. A fronte della maggiore circolazione delle informazioni che ne deriva (e del vantaggio che solo pochi soggetti, le grandi piattaforme, ne traggono), che si tratti o meno di una scelta consapevole e genuina non è in realtà la questione centrale. Il punto è che si vuole scoraggiare la concentrazione e l'accumulo di dati in capo a pochi soggetti, che potrebbero trarne indebiti vantaggi e porre in essere condotte fonte di rischio per la collettività.

Il controllo sulla validità del consenso ha dunque assunto funzioni che non gli competono ed è stato utilizzato in via strumentale per raggiungere obiettivi di restringimento del flusso delle informazioni. Il fallimento di tale strategia non stupisce, dato che non è il consenso individuale lo strumento adatto a gestire scelte sull'uso delle informazioni il cui impatto si produce non sui singoli ma su terzi o sulla collettività. Il risultato è stato quello di rendere estremamente difficile la raccolta di un valido consenso, considerando illecite tutte le modalità escogitate dalla prassi per incentivarlo (quali, ad esempio, le operazioni di *tying*), e incoraggiando al contrario l'adozione di modalità che inducano l'interessato a negare il consenso²⁸. Così, ad essere problematici sono i casi in cui, ad esempio, le caselle sono preimpostate sull'opzione positiva²⁹ o in cui la scelta di autorizzare il trattamento è presentata con colori più brillanti, mentre non lo sono quelli in cui ad essere

²⁶ Non è da escludersi infatti che il non interessarsi e il non prestare attenzione siano frutto di una scelta consapevole da parte dell'interessato che preferisca (comprensibilmente) dedicare ad altro il tempo e le energie necessari ad informarsi, evitando di leggere tutte le informative privacy che gli vengono sottoposte quotidianamente (il cui tempo di lettura è stato stimato, già anni fa, in 76 giorni l'anno: A.M. McDONALD, L.F. CRANOR, *The Cost of Reading Privacy Policies*, in *I/S A Journal of Law and Privacy for the Information Society*, 2008, 543 ss.). La scelta di non essere informato, purché si tratti di decisione consapevole, è d'altronde ammessa anche in campo medico (art. 1, co. 3, l. 219/2017), che costituisce uno degli ambiti in cui maggiore è l'attenzione verso una genuina manifestazione di volontà intesa in senso soggettivo.

²⁷ Per alcuni dati empirici su tale preferenza, v. N. JENTZSCH, S. PREIBUSCH, A. HARASSER, *Study on monetising privacy: An economic model for pricing personal information*, report per European Network and Information Security Agency, 2012.

²⁸ V. A. ACQUISTI, *Nudging Privacy: The Behavioral Economics of Personal Information*, in *IEEE Security & Privacy*, 2009, 82 ss.

²⁹ Tale modalità di raccolta del consenso è stata espressamente dichiarata illecita non solo dal Comitato europeo della protezione dei dati, ma anche dalla Corte di Giustizia dell'UE nei casi C-673/17, 1.10.2019 (caso Planet49), par. 52 e C-61/19, 11.11.2020 (caso Orange Romania), par. 37.

preimpostate siano le caselle sull'opzione negativa, oppure in cui le impostazioni del browser siano programmate nel senso di escludere l'installazione dei *cookies*.

In tal modo si producono però distorsioni rispetto alla questione regolatoria principale riguardante l'uso delle informazioni. Si è visto che le decisioni in merito a trattamenti che non hanno un impatto diretto e percepibile sull'interessato sono estremamente suscettibili al contesto e facilmente manipolabili. Se è vietato spingere verso una scelta positiva, mentre sono ammessi (e anzi richiesti) incentivi verso una scelta negativa, allora il rischio è quello di una restrizione del flusso delle informazioni senza tenere conto del fatto che, a prescindere dal consenso, potrebbe esserci un legittimo interesse a usare quei dati. Questo può portare a una non meditata restrizione della circolazione informazioni, che peraltro, viste le limitate capacità delle autorità di controllo, rischia di operare solo nei (relativamente pochi) casi che cadono sotto il loro scrutinio e, al di fuori di questi, di avere un effetto di deterrenza idoneo a colpire principalmente chi non ha i mezzi per affrontare le eventuali conseguenze sanzionatorie delle proprie condotte³⁰.

Si noti che il problema non si potrebbe risolvere imponendo condizioni neutre di prestazione del consenso, che non inducano né in una direzione né nell'altra (ad esempio, laddove per la validità del consenso si ritenessero illegittime le caselle preselezionate sia in un senso che nell'altro): in tal caso il rischio è che gli interessati, inconsapevoli oppure incuranti delle conseguenze su larga scala dei trattamenti, compiano scelte del tutto casuali o comunque dettate da sensibilità contingenti. Che tal fatta di decisioni costituisca il criterio principale per ammettere o meno l'uso delle informazioni sarebbe segno di una rinuncia da parte dell'ordinamento a regolare la questione.

3. Il consenso come strumento per facilitare l'uso dei dati

Non sembra tuttavia che il legislatore europeo sia intenzionato ad abdicare alla sua funzione di disciplinare l'uso delle informazioni. Esso, preso atto del potenziale dei dati per lo sviluppo tecnologico, economico e sociale, sta virando da un approccio basato sulla minimizzazione a una maggiore apertura verso la condivisione delle informazioni. Tale evoluzione è chiaramente affermata dalla Commissione europea che ha sottolineato il valore dei dati e auspicato la creazione di un "contesto politico attraente" per lo sviluppo dell'economia dei dati³¹. Non è chiaro quanto si tratti di un vero e proprio

³⁰ I titolari di più piccole dimensioni sono infatti naturalmente portati ad atteggiamenti precauzionali più marcati per tutelarsi da un legislatore spesso percepito come vessatorio. In reazione a ciò, si veda infatti la recente proposta volta a estendere misure di semplificazione in favore delle imprese c.d. small-mid cap: Commissione europea, *Proposal for a regulation concerning the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures*, COM(2025) 501 final, 21.5.2025.

³¹ Comunicazione della Commissione europea, *Una strategia europea per i dati*, COM(2020) 66 final, 19.2.2020. La necessità di facilitare il trattamento di grandi quantità dei dati personali si è fatta sentire in maniera particolarmente urgente con riguardo allo svi-

cambiamento di rotta rispetto al precedente atteggiamento: il percorso del legislatore sembra infatti essere quello di un progressivo affinamento nell'individuazione del punto di bilanciamento tra i contrapposti interessi a un uso più ampio o più ristretto delle informazioni, tramite l'introduzione di disposizioni man mano più specifiche che declinano in determinati ambiti i principi generali già affermati nel GDPR. A tal proposito i molteplici interventi legislativi che sono in seguito intervenuti hanno dato luogo a un quadro normativo frastagliato e poco coordinato, dal quale sembrano però emergere alcune direttrici che rendono ancora più evidente come il consenso sia da leggersi come strumentale rispetto a obiettivi più ampi³².

Innanzitutto il legislatore europeo ha in alcuni casi reso esplicitamente irrilevante l'eventuale prestazione del consenso, vietando determinate operazioni di trattamento a prescindere dalla presenza o meno di una manifestazione di volontà dell'interessato. Così, si è vietato alle piattaforme online di utilizzare le categorie particolari di dati o i dati dei minori per presentare pubblicità basata sulla profilazione (art. 26, par. 3 e art. 28, par. 2, Reg. UE 2022/2065) e sono state proibite le operazioni di *targeting* politico e di consegna del messaggio pubblicitario politico che comportano il trattamento di categorie particolari di dati personali o il trattamento di dati di soggetti al di sotto di una certa soglia di età (art. 18, par. 1, lett. c e par. 2, Reg. UE 2024/900)³³. Si noti che la prestazione del consenso è stata resa irrilevante non in ragione delle particolari difficoltà nei casi in questione a raccogliere un consenso consapevole e genuino, ma per evitare le conseguenze particolarmente rischiose per i singoli e per la collettività di alcuni trattamenti³⁴. Il legislatore ha inoltre talvolta disciplinato non le operazioni di trattamento ma i comportamenti che possono essere adottati a valle di esse: si pensi a tal proposito alla regolamentazione della immissione sul mercato e dell'utilizzo dei sistemi di intelligenza artificiale (Reg. UE 2024/1689), sviluppatasi e funzionanti proprio grazie all'ampia disponibilità di dati.

Nei casi in cui invece il trattamento dei dati è visto con favore, in quanto foriero di benefici per la collettività, allora il legislatore europeo si sta muovendo per facilitare l'uso dei dati o eliminando il consenso dalle basi legittimanti (e ammettendo il trattamento in virtù di un'altra condizione di liceità declinata in termini più specifici rispetto al generico legittimo interesse), oppure sostituendo la prestazione del consenso con un meccanismo di *opt-out* da parte degli interessati. Questa sembra essere la linea su cui sta operando il legislatore nella creazione degli spazi comuni europei di dati, definiti come "spazi interoperabili comuni di dati a livello dell'UE in settori strategici" che "mirano a superare gli ostacoli giuridici e tecnici alla condi-

luppo di sistemi di intelligenza artificiale, il quale, per l'appunto, dipende da un'ampia disponibilità di dati: v. in proposito già la Comunicazione della Commissione, *L'intelligenza artificiale per l'Europa*, COM(2019) 237 final, 24.4.2018, 10 ss.

³² Cfr. D. POLETTI, *Il controllo dell'interessato e la strategia europea sui dati*, in *Oss. fonti*, 2023, 367 ss.

³³ Il legislatore ha anche vietato alle piattaforme c.d. *gatekeeper* di combinare o utilizzare in maniera incrociata i dati provenienti da servizi diversi (art. 5, par. 2, lett. a, b, c, Reg. UE 2022/1925), ma ha reso tale divieto superabile da un consenso specifico dell'interessato.

³⁴ Non si tratta dunque di un atteggiamento paternalistico: Y. HERMSTRÜWER, *op. cit.*, 15 s.

visione dei dati tra le organizzazioni”³⁵. Tra tali ostacoli figura evidentemente anche la necessità di chiedere sempre il consenso dell’interessato, frutto in parte delle distorsioni di cui si è detto³⁶. Emblematico a tal proposito è il recente Reg. UE 2025/327 sullo spazio europeo dei dati sanitari, che disciplina la condivisione di tale tipologia di informazioni per finalità primarie e secondarie. In entrambi i casi non è previsto che l’interessato presti il proprio consenso, salvo il suo diritto di *opt-out*³⁷. Si noti che in questo caso, in cui l’obiettivo è esplicitamente quello di favorire l’uso dei dati, l’eventuale inconsapevolezza dell’interessato (estremamente probabile nel caso dell’*opt-out*) non è considerata problematica.

In tutti i casi sopra menzionati il ruolo del consenso dunque si riduce: o per impedire che esso possa giustificare trattamenti rischiosi o, al contrario, per dare spazio a una maggiore condivisione dei dati. Per raggiungere tale ultima finalità, il legislatore ha introdotto, in parallelo alle disposizioni che riducono la rilevanza del consenso in casi specifici, alcune previsioni di carattere più generale volte a facilitare e incentivare la prestazione del consenso da parte degli interessati. Il riferimento è alle disposizioni in merito all’altruismo e agli intermediari dei dati contenute nel Data Governance Act (Reg. UE 2022/868, DGA). Tali previsioni, pur senza apparentemente toccare la disciplina sul consenso contenuta nel GDPR e mantenendolo tra le basi legittimanti il trattamento³⁸, creano alcune frizioni rispetto alle interpretazioni sinora prevalenti dei requisiti del consenso al trattamento, frutto, come abbiamo detto, di un’impostazione volta a restringere il flusso delle informazioni (mentre il dichiarato scopo degli interventi legislativi in questione è quello di facilitare la circolazione dei dati).

Per quanto riguarda l’altruismo dei dati, definito come la condivisione volontaria dei dati per obiettivi di interesse generale, il legislatore europeo

³⁵ Commissione europea, *Una strategia europea per i dati*, cit., 17.

³⁶ E frutto anche, in taluni casi, di scelte restrittive da parte dei legislatori nazionali negli spazi lasciati liberi dal GDPR: emblematico è il caso dei trattamenti per finalità di ricerca medico-scientifica, per il quali l’ordinamento italiano detta una complessa disciplina che vede come regola generale l’obbligo di chiedere il consenso dell’interessato. In tema v. P. AURUCCI, *Il trattamento dei dati personali nella ricerca biomedica. Problematiche etico-giuridiche*, Napoli-Torino, 2022, 191 ss.

³⁷ Mentre per il trattamento per finalità secondarie l’*opt-out* è stabilito direttamente dal legislatore europeo, per il trattamento per finalità primarie esso è previsto solo se introdotto dai singoli Stati membri (art. 10). Questo non significa peraltro negare all’interessato un controllo sui propri dati, che è assicurato tramite il riconoscimento di vari diritti tra cui quello di accesso, di informazione, di rettifica e di limitazione (art. 3 ss.). Per quanto riguarda l’uso secondario, la tutela è offerta (i) dal divieto di utilizzare i dati per determinate finalità (in particolare, per adottare decisioni pregiudizievoli per una persona fisica o per un gruppo di persone fisiche, per svolgere attività pubblicitarie o di marketing, per sviluppare beni o servizi che possano danneggiare le persone, la salute pubblica o la società in generale e per attività contrarie all’ordine pubblico, art. 54) e (ii) dalle modalità con cui la condivisione deve essere attuata, sempre intermediata da un organismo pubblico. L’unico caso in cui si prevede la necessità dell’*opt-in* dell’interessato è per l’utilizzo per finalità secondarie dei dati raccolti tramite le applicazioni per il benessere, considerata l’invasività di tale raccolta rispetto alla sfera privata delle persone. In tema cfr. M.S. ESPOSITO, *Tutela dei dati personali e ricerca scientifica in ambito sanitario: il GDPR e il Regolamento sullo spazio europeo dei dati sanitari (EHDS)*, in *Jus civile*, 2024, 932 ss.

³⁸ V. art. 1, par. 3, DGA.

ha chiaramente esplicitato l'obiettivo di incentivare la prestazione del consenso tramite la predisposizione di strumenti di facile utilizzo affinché gli interessati possano condividere i propri dati e attraverso l'organizzazione di campagne di sensibilizzazione per informare sui benefici e i vantaggi di tali operazioni di trattamento (considerando 45, DGA). Si noti la distanza rispetto a quanto affermato finora dalle autorità di controllo in merito al consenso, la cui libertà rischia di essere inficiata da qualsiasi richiamo emotivo³⁹. Laddove lo scopo sia quello di facilitare la circolazione dei dati, sembrano invece aprirsi spazi di liceità per alcune pratiche di *nudging* sinora guardate con sospetto. Un altro allentamento dei requisiti del consenso potrebbe aversi con riguardo alla specificità. Il Comitato europeo per la protezione dei dati ha sinora escluso la validità del c.d. *broad consent* (specie laddove siano in gioco dati sensibili)⁴⁰, il quale, in particolare nell'ambito della ricerca scientifica, consentirebbe di raccogliere un consenso valido per interi settori di ricerca (e non per una specifica ricerca dettagliatamente descritta) e che potrebbe essere particolarmente utile per i trattamenti volti a finalità altruistiche. Una lettura meno restrittiva pare però suggerita dallo stesso legislatore, che afferma esplicitamente che le “finalità di ricerca scientifica potrebbero essere sostenute dal consenso in determinati settori di ricerca scientifica” (considerando 50, DGA)⁴¹.

Per quanto riguarda invece gli intermediari dei dati⁴², i quali offrono servizi “che mira[no] a instaurare, attraverso strumenti tecnici, giuridici o di al-

³⁹ EDPB, *Linee guida 03/2022*, cit., 75, in cui sono qualificati come ingannevoli i richiami emotivi (*emotional steering*) quali, ad esempio, “Raccontaci di te! Forza, non vediamo l'ora di conoscerti!”, oppure “i tuoi amici si dimenticheranno di te” nel caso di disattivazione dell'account. Lo stesso utilizzo del termine “altruismo” dei dati sembra volto a presentare la condivisione dei dati in una luce positiva, come pratica benefica per il prossimo.

⁴⁰ EDPB, *Linee guida 5/2020*, cit., p. 33 s., in cui, pur dando atto della maggiore flessibilità consentita dal considerando 33 del GDPR, quando la ricerca coinvolge categorie particolari di dati (dunque, in pratica, nella quasi totalità della ricerca in ambito medico), il Comitato esclude che la finalità possa essere indicata in termini ampi e ammette unicamente un consenso a fasi progressive (c.d. consenso dinamico). Un atteggiamento in proposito cauto è stato adottato anche dal Garante europeo della protezione dei dati, *A preliminary Opinion on data protection and scientific research*, 6.1.2020, p. 19. Su tale posizione restrittiva v. P. AURUCCI, *op. cit.*, 168 ss. Invece di ammettere allentamenti dei requisiti del consenso, il Comitato europeo ha invitato piuttosto a considerare l'opportunità di usare, per la ricerca scientifica in ambito medico, una base giuridica diversa dal consenso stesso: EDPB, *Parere 3/2019 relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati*, 23.1.2019.

⁴¹ Si noti che identica espressione è adottata al considerando n. 33 del GDPR, la quale tuttavia è stata oggetto di interpretazione restrittiva da parte delle autorità di controllo (v. la nota che precede). Sulla coincidenza tra i considerando dei due diversi regolamenti v. D. SBORLINI, *The broad consent as a means for the valorization of personal data in the field of scientific research and its relief in the spaces of data sharing*, in *Contr. impr.*, 2024, 223 ss. Bisognerà dunque vedere se la reiterazione dell'espressione in questione anche nel Reg. EU 2022/868, improntato a un maggiore favore verso la condivisione dei dati, porterà a una diversa interpretazione: interessanti indicazioni potranno probabilmente ricavarsi dal modulo europeo di consenso all'altruismo dei dati che la Commissione è tenuta a redigere (art. 25, Reg. UE 2022/868).

⁴² Su cui v. D. POLETTI, *Gli intermediari dei dati*, in *European Journal Priv. Law Tech.*, 2022, 45 ss.; A. OWUSU, *Data Sharing in the Personal Data Economy. Does Sharing Mean Caring?*, *ivi*, 2023, 217 ss.

tro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati [...]” (art. 2, n. 11, DGA), ci si può chiedere se esso conduca a una rivisitazione del requisito della libertà del consenso sotto il profilo della presunta incommerciabilità dei dati personali così come affermata dalle autorità di controllo⁴³. Sicuramente la norma non esclude espressamente la possibilità per gli interessati di ricevere una remunerazione per l’utilizzo dei propri dati e, anzi, uno dei possibili (e auspicati) effetti positivi della diffusione degli intermediari dei dati è anche quella di redistribuire la ricchezza proveniente dal trattamento dei dati consentendo anche agli interessati di trarne un beneficio. Se la ragione alla base del presunto divieto di commerciabilità diretta da parte degli interessati è quello di evitare gli abusi derivanti dallo squilibrio di potere nel rapporto tra titolari e interessati, allora la disciplina sugli intermediari dei dati non dice nulla di nuovo ma è anzi volta proprio ad affrontare tale problema. Le norme in questione sono invece più difficilmente compatibili con l’idea (fatta propria dai garanti) secondo cui l’incommerciabilità deriverebbe dalla natura dei dati quali oggetto di diritti fondamentali della personalità.

Il legislatore europeo apre dunque a una rivisitazione della nozione e dei requisiti del consenso dell’interessato nell’ottica di facilitare l’uso dei dati; starà tuttavia agli interpreti cogliere o meno tali aperture.

Si noti che, parallelamente al legislatore, anche le autorità di controllo stanno iniziando a mostrare una maggiore attenzione verso basi legittimanti diverse dal consenso (mantenendo invece un atteggiamento estremamente rigido con riguardo a quest’ultimo), e un pari interesse è prestato dagli attori di mercato che, resisi conto della difficoltà a raccogliere un valido consenso, si muovono alla ricerca di altre condizioni di liceità⁴⁴.

A suon di sanzioni, alcuni importanti titolari del trattamento, preso atto della difficoltà di ottenere un consenso valido, hanno infatti reputato più prudente avvalersi di una base giuridica diversa⁴⁵. Se non è lecito preimporre il consenso al trattamento dei dati né subordinare l’erogazione di un servizio alla prestazione del consenso, se la scelta di negare il consenso non deve essere più difficile di quella di prestarlo, allora il timore è che gli interessati (non indotti in alcun modo ad acconsentire) dicano di no, impedendo in tal modo la raccolta dei dati: meglio allora assicurarsi di poter trattare i

⁴³ 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*, 14.3.2017.

⁴⁴ Non siamo in grado di dire quanto le previsioni sui requisiti del consenso siano effettive ed efficaci nel garantire la consapevolezza degli interessati (probabilmente poco); esse non sono però più percepite come innocue da parte dei titolari del trattamento tanto quanto lo erano in passato e d’altronde, basta l’esperienza quotidiana a confermare come nel tempo le richieste di prestare il consenso siano cambiate, consentendo di esprimere più facilmente un rifiuto.

⁴⁵ Corte di Giustizia UE, C-252/21, 4.7.2023 (caso Meta Platforms), in cui Meta, pur di non doversi avvalere del consenso dell’interessato, ha (senza successo) invocato la sussistenza di quasi tutte le altre condizioni di liceità: l’esecuzione di un contratto (ma la Corte non ha ritenuto che il trattamento fosse indispensabile a tale fine), l’interesse pubblico (escluso “data la natura e il carattere essenzialmente economico e commerciale della sua attività”) e il legittimo interesse (escluso anch’esso per il trattamento finalizzato alla personalizzazione della pubblicità a fronte della estensione dei dati raccolti e delle aspettative degli utenti).

dati sulla base di un'altra condizione legittimante. In questi casi l'attenzione si sposta dal consenso al legittimo interesse e l'allargamento o la restrizione del flusso delle informazioni dipende non più dalla facilità a raccogliere il consenso, ma da come si intende il legittimo interesse, con il quale gli interpreti hanno dunque avuto modo di iniziare a confrontarsi in maniera più diretta. Questo permette di affrontare il problema se ammettere o meno l'uso dell'informazione senza mascherarlo dietro all'invalidità (fin troppo facile da rilevare) dei consensi individuali. Emergono soluzioni interessanti: così, da un lato si è escluso che il legittimo interesse giustifichi raccolte massive di dati usati per sviluppare e migliorare un servizio quando si tratta della personalizzazione di contenuti per scopi di marketing⁴⁶, mentre si è ammesso, seppur cautamente, il possibile operare del legittimo interesse quando il trattamento è necessario ad allenare sistemi di intelligenza artificiale⁴⁷. L'esame di tali soluzioni fuoriesce dal presente contributo: qui interessa solo evidenziare come, tolta rilevanza al consenso, gli interessi in gioco emergano con maggiore chiarezza.

4. I compiti impropri del consenso

Provando a riannodare i fili di quanto sinora detto, torniamo alla domanda di partenza sul senso di continuare ad annoverare il consenso dell'interessato tra le basi legittimanti il trattamento dei dati personali. Tale previsione è problematica solo se si attribuiscono al consenso compiti che non gli competono.

Il primo tra questi compiti è quello di offrire tutela contro i rischi dei trattamenti. Lo stesso legislatore non ritiene che tale funzione possa essere assolta attraverso la necessità di una manifestazione di volontà degli interessati. Le previsioni sui requisiti del consenso si affiancano infatti a una serie di misure volte a proteggere i dati qualunque sia la base legittimante il trattamento (e dunque anche se un consenso c'è stato): chi tratta i dati deve in ogni caso fare una valutazione del rischio del trattamento e adottare tutte le misure adeguate a fronteggiare i rischi posti dallo specifico trattamento posto in essere⁴⁸, fatti salvi, in ogni caso, i principi generali con riguardo alla minimizzazione, alla limitazione delle finalità e alla sicurezza. La dimensione effettiva della protezione dei dati risiede in tali misure: quando si insiste sull'inidoneità del consenso a tutelare gli interessati, non ci si deve dimenticare che la normativa è ben lontana dal fare del consenso il principale strumento di protezione⁴⁹.

Il secondo di questi compiti impropri è, come si è visto, quello di regolare il flusso delle informazioni. Al di fuori dei casi in cui vi sono effettive

⁴⁶ Corte di Giustizia UE, caso Meta Platforms, cit.

⁴⁷ EDPB, *Report of the work undertaken by the ChatGPT Taskforce*, 23.5.2024.

⁴⁸ V. artt. 24, 25, 32, 35 e 36, GDPR.

⁴⁹ Senza contare che il consenso non vale a legittimare un trattamento vietato da altre norme dell'ordinamento: S. ORLANDO, *Consenso al trattamento e liceità*, in *Pers. merc.*, 2024, 333 ss. Sulla necessità di spostare il problema dalla sfera individuale a una più ampia e collettiva, v. I.A. Caggiano, *op. cit.*, 48 ss.

esigenze di garantire l'autodeterminazione informativa, come quando il trattamento ha un impatto diretto sull'interessato, questa funzione non può utilmente essere assolta dal consenso ma dalla precisa individuazione da parte del legislatore delle altre basi legittimanti il trattamento. Abbiamo detto che le alternative spaziano da una circolazione libera a una controllata. Nella prima prospettiva, al fine di mantenere in piedi adeguate tutele, occorrerebbe però irrobustire le garanzie a valle del trattamento, intervenendo direttamente sui rischi posti dalle operazioni di trattamento per così dire liberalizzate a monte⁵⁰. Nella seconda, occorrerebbe invece che il legislatore effettui scelte chiare, precise ed esaustive su quali sono i casi in cui i dati possono essere utilizzati, pena il rischio di restrizioni o allargamenti eccessivi della circolazione dei dati. Togliere rilevanza al consenso, per quanto possa essere opportuno, senza però contemporaneamente definire le condizioni a cui i dati possono essere utilizzati rischia in altre parole di lasciare una disciplina pericolosamente monca. Il legislatore europeo pare essere di ciò consapevole e, difatti, quando ha introdotto norme che riducono la rilevanza del consenso, lo ha fatto con riguardo a settori determinati, in cui gli utilizzi consentiti dei dati sono indicati con maggiore specificità (come per gli spazi comuni di dati), e ha accompagnato tali disposizioni con altre volte ad affrontare direttamente i trattamenti più rischiosi introducendo specifiche garanzie.

Al di fuori (lo si ripete) dei casi in cui occorre tutelare l'autodeterminazione informativa dei singoli, la congruità delle norme che prevedono e disciplinano il consenso va dunque valutata con riferimento alla loro idoneità non a garantire una manifestazione di volontà attenta e consapevole (obiettivo che resta in realtà in secondo piano)⁵¹, ma ad assicurare una circolazione dei dati coerente con le linee di politica del diritto che guidano il legislatore europeo nella costruzione di un'economia basata sui dati che non rinunci alla tutela dai rischi posti dai trattamenti massivi. In quest'ottica il problema principale diventa quello di individuare con chiarezza gli obiettivi ordinamentali, individuazione non sempre agevole in un contesto, come quello in esame, in cui il legislatore europeo, nel tentativo di non scontentare nessuno, effettua equilibrismi normativi che conducono all'adozione di disposizioni ambigue e poco chiare che hanno lasciato spazio al perseguimento da parte delle autorità di controllo di una politica del diritto sostanzialmente autonoma.

⁵⁰ V. S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *Media Laws*, 2019, 147;

⁵¹ Cfr. D.J. SOLOVE, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, in *Boston University Law Rev.*, 2024, 631, laddove propone di riconoscere apertamente la natura fittizia del consenso, accettandola come una menzogna necessaria a far funzionare l'economia digitale.

