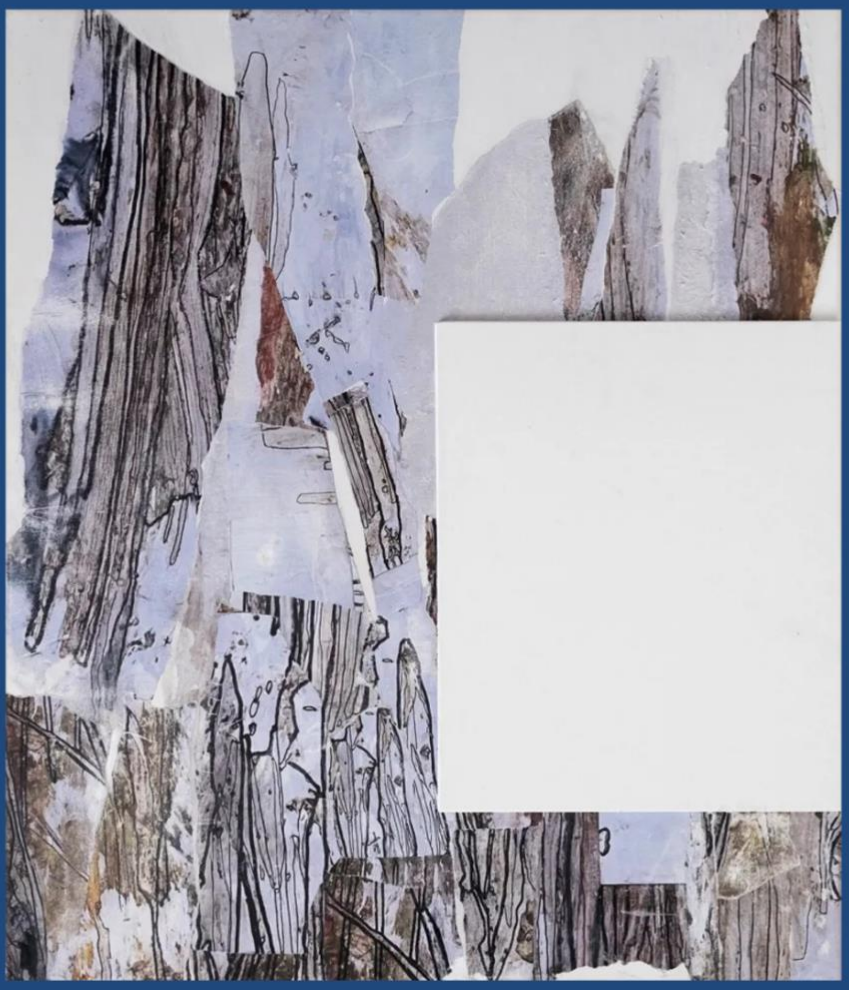
PERSONA E MERCATO
Dialoghi sul nostro tempo



Libertà e liceità del consenso nel trattamento dei dati personali

A cura di Salvatore Orlando

***Libertà e liceità del consenso nel trattamento dei dati personali*, a cura di Salvatore Orlando, Persona e Mercato ed., Firenze, 2024**

ISBN 978-88-947441-3-2

In copertina, riproduzione dell'opera *Deriva (fig.5)*, 2021, tecnica mista su tela, di Domenico D'Orsogna, collezione privata. Tutti i diritti riservati.

Il curatore ringrazia il dott. Riccardo Alfonsi per il suo prezioso lavoro editoriale.

a Dianora Poletti

PRESENTAZIONE

Il volume raccoglie l'elaborazione scritta, integrata e corredata di note, degli interventi svolti dagli autori al Convegno *Libertà e liceità del consenso nel trattamento dei dati personali* svoltosi a Firenze il 5 maggio 2023, organizzato dalla rivista *Persona e mercato* e dall'OGID (Osservatorio giuridico sull'innovazione digitale).

I contributi hanno ad oggetto il tema centrale del c.d. consenso *privacy* nel contemporaneo contesto della *data economy*, analizzato sotto diversi angoli visuali: la libertà, il contratto, la liceità, il rapporto con le c.d. decisioni algoritmiche, i problemi di tutela dei diritti fondamentali e di giustizia contrattuale, visti anche sotto la lente della giurisprudenza europea.

Il volume, così come, prima di esso, il Convegno, si fregiano delle preziose relazioni del Presidente e della Vice Presidente dell'Autorità Garante per la protezione dei dati personali, Prof. Pasquale Stanzione e Prof.ssa Ginevra Cerrina Feroni.

Il curatore e gli autori lo tributano alla memoria di Dianora Poletti, che parlò al Convegno, da par suo, della giurisprudenza della Corte di Cassazione su un tema tanto attuale.

Settembre 2024
Il curatore

INDICE

INTRODUZIONE

Di Pasquale Stanzione

Sono doppiamente lieto (come Presidente del Garante e come civilista) di discutere oggi – e con così autorevoli Relatori – di un tema tanto rilevante per la protezione dei dati, come il consenso al trattamento. È, infatti, quantomai opportuno promuovere una riflessione su questo punto, in un momento, quale quello attuale, in cui sono incessanti e significativi i mutamenti nel contesto socio-economico di riferimento, cui le categorie giuridiche (*queste* categorie giuridiche) si applicano.

Il consenso al trattamento è, sotto questo profilo, emblematico dell'interrelazione tra innovazione e regolazione: esso, infatti, è stato tradizionalmente concepito come massima espressione della *privacy* quale autodeterminazione informativa: manifestazione non soltanto di volontà ma anche del potere di autonoma decisione dell'interessato, in ordine all'ambito circolatorio ammesso per i suoi dati. La disciplina italiana previgente assegnava al consenso un ruolo centrale, al punto da concepire la maggior parte degli altri presupposti di liceità del trattamento come specifiche esimenti. La sostanziale equivalenza dei presupposti di liceità nel GDPR smentisce, soltanto apparentemente, questa primazia.

Lo statuto giuridico peculiare accordato al consenso al trattamento (ben più pregnante del consenso negoziale), con i suoi requisiti di libertà, specificità, granularità, previa informazione, inequivocabilità, revocabilità *sine die* e *ad nutum*, ben chiariscono, infatti, come neppure la pluralità di basi giuridiche nel GDPR determini una reale dequotazione del consenso. La stessa sua libertà non va intesa, riduttivamente, come assenza di coartazione ma, anche, come assenza di condizionalità significativa, tale cioè da incidere fortemente sul processo motivazionale del soggetto.

Alla luce delle riforme recenti (*Data Governance Act*, in particolare) è il consenso a governare istituti profondamente innovativi come l'altruismo dei dati, che potrà svolgere un ruolo importante nella destinazione solidaristica dei dati personali. Il formante pretorio ha, poi, ulteriormente valorizzato il requisito dell'inequivocabilità, soprattutto rispetto ai *dark patterns* tipici del web, desumendone ad esempio l'invalidità della preimpostazione dell'assenso (si vedano, al proposito, le decisioni della Corte di Giustizia dell'Unione Europea nei casi c.d. 'Planet 49' e 'Orange c. Romania').

La giurisprudenza di legittimità interna (sviluppando le posizioni del Garante) ha, per altro verso, valorizzato la natura informata e specifica del consenso, esigendone ad esempio una rinnovazione nel caso di mutamento del titolare (caso c.d. 'Tiziana Life') o, per altro verso, l'informazione in ordine al tipo di logica applicata a un algoritmo per il *rating* reputazionale delle persone (caso c.d. 'Mevaluate').

L'attenzione riservata, tanto dalla Corte di giustizia quanto dal legislatore europeo, ai requisiti di effettiva libertà e consapevolezza del consenso dimostra quanto l'autodeterminazione informativa sia determinante per un governo sostenibile della società (e dell'economia) delle piattaforme.

Ma è ancora possibile garantire l'effettiva autodeterminazione del soggetto e, quindi, un suo reale potere decisionale in un contesto socio-economico caratterizzato dal rischio di un

sostanziale svuotamento della funzione del consenso, di fronte a trattamenti dalle implicazioni poco comprensibili e dalla solo apparente gratuità delle 'transazioni' *online*?
Da un lato, infatti, la *consent fatigue*, unitamente alla crescente complessità (e numerosità) dei trattamenti da autorizzare rischia di svalutare la funzione del consenso, facendolo percepire come un inutile adempimento privo di reale significato. Per questa ragione, ad esempio, il *draft* di regolamento *e-privacy* interviene con misure semplificatorie rispetto al consenso da prestare in relazione ai *cookies*.
Per altro verso, si assiste a una tendenza alla sempre più frequente connotazione del consenso in senso condizionale e non opzionale. Lo schema dati-contro-servizi costituisce, infatti, una fattispecie ricorrente - forse addirittura la più diffusa - in un'economia, come quella attuale, *data driven*. Tanto ciò è vero che la direttiva sui contenuti digitali (ma anche la *omnibus)* estende le tutele consumeristiche ai contratti in cui, a fronte della fornitura di contenuti o servizi (in particolare digitali), il consumatore fornisca i propri dati personali, diversi e ulteriori rispetto a quelli necessari all'esecuzione del contratto o all'adempimento di obblighi di legge.
Nel recepire le indicazioni del Garante europeo per la protezione dei dati, entrambe le direttive si curano di non definire espressamente (come invece la n. 2019/770 definiva originariamente) i dati quali controprestazione. Tuttavia, di là da questa modifica per lo più di *drafting* e, certo, di lessico normativo, la semantica non cambia: si riconduce, tra le fattispecie contrattuali, quelle fondate sullo scambio servizi-contro-dati, pur prescrivendo come inevitabile il rispetto della disciplina di protezione dei dati (tra cui il carattere informato della manifestazione di volontà).
La soluzione normativa non deve, peraltro, stupire considerando che già la Cassazione (sia pur ragionando nell'ottica della direttiva-madre), con la sentenza sul caso c.d. '*Adspray*' n. 17278 del luglio 2018, negando che l'ordinamento vieti lo scambio di dati personali, ha però ribadito l'esigenza che esso sia il "frutto di un consenso pieno ed in nessun modo coartato", ulteriore e diverso rispetto a quello contrattuale. La Corte ha, peraltro, precisato come le operazioni di *tying* siano vietate (solamente) se la prestazione è "ad un tempo infungibile ed irrinunciabile per l'interessato".
Si sono, insomma, indicati come limiti di ammissibilità di quello schema la fungibilità della prestazione e l'assenza di reale pregiudizio derivante dalla rinuncia ad essa, con la previsione implicita, dunque, di requisiti ulteriori e diversi da quelli dei vizi della volontà contrattuale, assimilabili più ai presupposti per la rescindibilità del contratto.
La Cassazione coglieva dunque, già nel vigore della disciplina di protezione dei dati precedente, il vero tema sotteso alla diffusione di questo schema economico: l'esigenza di impedire l'elusione delle garanzie per l'autodeterminazione informativa, suscettibile di derivare dall'assimilazione, a una prestazione qualunque, del consenso al trattamento dei dati personali.
Si potrà discutere – e si discute – dell'ammissibilità di una dissociazione dell'*ownership* sul dato dalla vera e propria monetizzazione del consenso, chiedendosi se sia possibile, come per il *copyright*, ammettere una circolazione fondata su di un modello remunerativo parallelo alla persistenza di diritti extrapatrimoniali sul dato stesso.
Ciò che è certo è che bisogna avere chiara la posta in gioco. In assenza di un controllo effettivo sull'assenza di coartazione del consenso, infatti, si rischia di legittimare lo sfruttamento delle condizioni di debolezza (non solo economica, ma anche cognitiva) che possono caratterizzare alcuni ceti sociali, ricreando di fatto un vero e proprio sottoproletariato nelle maglie del capitalismo digitale.
La questione diviene ancora più complessa nel caso dei dati appartenenti a categorie particolari, come anche quelli biometrici, che espongono l'interessato a scelte ancora più difficili in ragione dei rischi connessi alla prestazione del consenso. Si pensi al caso riportato dalla stampa alcuni anni fa secondo cui una nota azienda dei GAFAM, per 'allenare' i propri sistemi di

riconoscimento facciale, avrebbe offerto 5 dollari a coloro che, preferibilmente *homeless*, e di pelle scura, fossero stati disposti a offrire l'immagine del proprio volto da scansionare.
In ogni caso, i limiti che caratterizzano il consenso al trattamento dei dati e la sua tenuta nel contesto socio-economico attuale ben possono suggerire l'opportunità di rafforzare anche, in via preventiva, le misure di garanzia della correttezza del trattamento, ampliative del grado di responsabilizzazione del titolare e, parallelamente, la *liability rule* almeno per le attività massive come, ad esempio, quelle proprie delle piattaforme.
Sono temi, questi, sui quali va aperto un dibattito il più possibile ampio e 'laico', privo di precomprensioni e auspicabilmente lungimirante. Dai relatori e dalle relatrici di questa mattina, ai quali cedo subito la parola, attendiamo dunque sollecitazioni e suggestioni sicuramente preziose.

IL RUOLO DEL CONSENSO E L'INTERESSATO VULNERABILE

Di Ginevra Cerrina Feroni

SOMMARIO*: *1. La centralità del consenso privacy e il cambio di paradigma post GDPR. - 2. La posizione di debolezza dell'individuo che presta il consenso. - 3. L'Autorità e i nuovi confini del consenso. - 4. Contestualizzazione dei nuovi orizzonti del consenso nelle dinamiche contemporanee. - 5. Consenso: un'evoluzione del concetto di consenso e coesistenza con pratiche negoziali sul dato personale.

1. La centralità del consenso privacy e il cambio di paradigma post GDPR.

Per molti anni il consenso è stato il pilastro centrale della normativa in materia di protezione dei dati personali. L'idea sottostante era dare preminenza alla volontà e autonomia decisionale della persona, basti pensare alle disposizioni della Direttiva 95/46/CE[1] che inquadrava il consenso come base giuridica preminente, prevedendo quelle ulteriori solo come residuali.
Tale concezione è stata trasposta anche in sede di recepimento della direttiva da parte del legislatore italiano. In tal senso, si consideri l'art. 23 D.Lg. 30.6.2003, n. 196[2], ora abrogato, che seguiva la suddetta impostazione. Il consenso al trattamento dei dati personali per determinate finalità si poneva, quindi, come presidio di autodeterminazione informativa, la massima espressione di una volontà, informata, specifica e, soprattutto, libera[3], ergo non coartata e nemmeno condizionata. La *ratio* di tale impostazione trovava il fondamento in una società nella quale la diffusione dei mezzi di *internet* non era ancora capillare e si riteneva che l'espressione di volontà conferita dagli utenti alle singole operazioni di trattamento potesse avvenire in misura consapevole e coerente al dettato normativo.
Con il diffondersi dei *social network* e delle numerosissime applicazioni *online*, le espressioni di volontà da rilasciare da parte del singolo utente sono aumentate esponenzialmente e, di conseguenza, il legislatore ha dovuto mettere in discussione il meccanismo del consenso quale preminente condizione di liceità. Infatti, con l'approvazione del GDPR[4] nel 2016, si è assistito ad un cambio di paradigma: per quanto concerne i cd. dati comuni, ossia non appartenenti a

[1] Dir. 95/46/CE del Parlamento Europeo e del Consiglio del 24.10.1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
[2] Cass., 2.7.2018, n. 17278: "L'art. 23 Codice Privacy reca uno dei principi fondanti della materia giacchè, anche per la collocazione sistematica della disposizione nel Titolo 3 del Codice, che pone le regole generali per il trattamento dei dati, sta a significare che il consenso è condizione - fatti salvi casi eccettuati che qui non rilevano - della liceità del trattamento, ponendosi in armonia con il dettato dall'art. 2, lettera h) della direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995, che definisce il consenso come «qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento", direttiva in cui si chiarisce ulteriormente, all'art. 7, che il trattamento dei dati personali può essere effettuato soltanto quando "la persona interessata ha manifestato il proprio consenso in maniera inequivocabile»".
[3] F. DI RESTA, *La nuova "Privacy europea". I principali adempimenti del regolamento UE 2016/679 e i profili risarcitori*, Torino, 2018, 72.
[4] Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio del 27.4.2016 (c.d. Regolamento generale sulla protezione dei dati o GDPR).

categorie particolari, il consenso ora rappresenta solo una delle possibili e alternative basi giuridiche[5].
Questo approccio si colloca all'interno del più ampio principio di *accountability*[6]: il titolare del trattamento, cioè la figura che detiene il potere di definire e perimetrare il trattamento dei dati personali che verrà posto in essere, ha l'onere, per il rispetto del principio di liceità ivi inteso, di determinare la base giuridica più idonea a fondamento del proprio operato, scegliendo la più opportuna tra quelle previste.
Con tale normativa non è stato introdotto un divieto, bensì si è stabilito un parametro di valutazione da considerare insieme ad altri ed altrettanti rilevanti che intervengono nel caso concreto. Lo scopo era proprio quello di non ridurre l'espressione di volontà a una mera e fittizia clausola di legittimità dell'altrui potere negoziale e tecnologico[7].
Quindi, in quanto parametro di validità rispetto a un'attività che coinvolge un diritto della personalità, il consenso si trova oggi ad operare su un piano nuovo, ulteriore e non sovrapponibile rispetto alla manifestazione della volontà negoziale di un utente che intende usufruire di un determinato servizio.
Passando ora alla disciplina post-GDPR, agli artt. 7 e 8, tale regolamento impone determinati requisiti affinché il consenso possa considerarsi validamente prestato: la persona deve essere adeguatamente informata circa il trattamento che verrà posto in essere; avere una effettiva, specifica e libera scelta; poter rifiutare o revocare il consenso senza subire un pregiudizio. Nel caso del consenso prestato da un soggetto minorenne, sono previste ulteriori condizioni di validità, data l'intrinseca fragilità dell'interessato in minore età, rispetto all'adulto.
Tali requisiti portano a desumere che il legislatore abbia voluto sposare una concezione del consenso inteso più come autorizzativo, sulla scorta della scriminante penale, che di natura contrattuale: un consenso che esprime non tanto la volontà, ma la personalità dell'interessato e che, dunque, in quanto tale, non possa avere natura patrimoniale[8]. Il consenso penale, infatti, rimuove un limite rispetto a un comportamento che altrimenti sarebbe illecito e, nei limiti stabiliti dall'ordinamento circa il diritto disponibile, lo rende consentito. Quello negoziale invece consente di dare seguito a un comportamento che sarebbe già di per sé lecito. Per questi motivi, il consenso penale ha requisiti più stringenti (art. 50 c.p.) che paiono più coerenti con quelli previsti dall'art. 7 GDPR. Peraltro, diversi provvedimenti del Garante[9] e diverse sentenze della giurisprudenza[10] hanno richiamato tale visione.
Un *focus* particolare, ai fini della validità, è poi posto sull'esigenza di presidiare una eventuale situazione di debolezza dell'interessato, in particolare sia sotto il profilo della evidente "asimmetria informativa" e della posizione di squilibrio tra questi e il titolare del trattamento, sia sul versante della tutela contro possibili tecniche commerciali aggressive.

2. La posizione di debolezza dell'individuo che presta il consenso

[5] M. BORGOBELLO, *Manuale di diritto della protezione dei dati personali, dei servizi e dei mercati digitali,* Milano, 2023, 189 ss.
[6] Art. 5, Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio del 27.4.2016.
[7] G. ALPA e G. RESTA, *Le persone e la famiglia.Vol.1:le persone fisiche e i diritti della personalità*, Torino, 2019, 128 ss.
[8] S. THOBANI, *I requisiti del consenso al trattamento dei dati personali*, Roma, 2016, 3 ss.
[9] Garante della protezione dei dati personali, Provvedimento correttivo e sanzionatorio nei confronti di TIM S.p.A., 15.1.2020, doc.web. n.9256486.
[10] Cass., 2.7.2018, n. 17278: "l'ordinamento non vieta lo scambio di dati personali, ma esige tuttavia che tale scambio sia frutto di un consenso pieno ed in nessun modo coartato".

Circa la debolezza inerente lo squilibrio di posizione, il considerando 43 GDPR[11], difatti, sottolinea che il consenso non si possa considerare fornito liberamente se, ad esempio, esiste un evidente squilibrio tra la persona e l'azienda/organizzazione (ad esempio nel rapporto tra datore di lavoro e il suo dipendente), o qualora un'impresa richieda alle persone il consenso al trattamento di dati personali non necessari come condizione per l'adempimento di un contratto o la fornitura di un servizio. Così pure non sarebbe valido il consenso prestato dal lavoratore perché reso in una condizione di squilibrio di potere contrattuale rispetto al datore di lavoro[12]. Così, ad esempio, il legislatore italiano ha escluso che il trattamento dei dati personali funzionale alla fruizione della prestazione di cura possa essere retto dal consenso perché, appunto, non sarebbe libero in quanto necessitato da esigenze primarie[13]. Circa la debolezza emergente dall'asimmetria informativa, è innegabile la vulnerabilità di alcuni individui dinanzi a tecnologie e trattamenti caratterizzati da un'ampia complessità informativa, e ciò può indurli a conferire i propri dati personali per ottenere un vantaggio economico dietro prestazione di un consenso che in realtà è solo apparentemente informato[14].
Choice, l'associazione per la difesa dei consumatori australiana, ha realizzato un video in cui il protagonista si cimenta nella lettura di tutte le 73.198 parole che compongono i termini e condizioni del lettore e-book Kindle prodotto da Amazon. L'esperimento evidenzia come per leggere tale contratto siano necessarie circa otto ore e 59 minuti[15], un quantitativo di tempo che pressoché nessuno può dedicare a tale attività. Nel 2016 anche l'associazione dei consumatori norvegesi ha letto in diretta sul proprio sito i termini e le condizioni delle 33 *app* più utilizzate dai loro connazionali tra cui: i-Tunes, Skype, Instagram, Twitter, YouTube, Facebook, Tinder, Whatsapp e Netflix per nominare alcune delle più famose, impiegando trentuno ore[16].
Quindi oggi il consenso è diventato necessario per poter accedere e usufruire della maggior parte dei servizi *online*, con il rischio di rimanere tagliati fuori da una fondamentale parte di socialità[17]. Allo stesso tempo, tuttavia, il consenso *privacy* risulta, alla luce del dato normativo, tale da non ammettere compressioni e incomprensioni di alcun genere, né sopportare di essere perturbato non solo per effetto di errore, violenza o dolo, ma dell'intero ventaglio di possibili disorientamenti, stratagemmi, opacità, sotterfugi, slealtà, doppiezze o malizie comunque adottate nella prassi attuale dai titolari del trattamento.

3. L'Autorità e i nuovi confini del consenso.

La linea di confine oggi diventa molto sottile e facilmente valicabile sottoponendo a dura prova il principio cardine dell'informato ed inequivocabile consenso; si pensi ai moduli o caselle di

[11] E. BELISARIO e G.M. RICCIO e G. SCORZA, *GDPR e normativa privacy. Commentario*, Milano, 2022.
[12] Gruppo di lavoro Articolo 29, Linee guida sul consenso ai sensi del Reg. (UE) 2016/679, adottate il 28 novembre 2017, come modificate e adottate da ultimo il 10 aprile 2018, 259 rev. 01., par. 3.1.1.
[13] S. ORLANDO, *Per un sindacato di liceità del consenso "privacy"*, in *Pers. merc.*, 2022, 537 ss.
[14] S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018, 161 ss.
[15] HuffPost Online, *Ecco quanto tempo impiegheresti a leggere termini e condizioni dei prodotti acquistati,* 2017, https://www.huffingtonpost.it/archivio/2017/03/17/news/ecco_quanto_tempo_impiegheresti_a_leggere_termini_e_condizioni_dei_prodotti_acquistati-5456845/.
[16] D. BERREBY, *Click to agree with what? No one reads terms of service, studies confirm*, The Guardian Online, 2017, https://amp.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print.
[17] A. ALONGI e F. POMPEI, *Diritto della privacy e protezione dei dati personali: Il GDPR alla prova della data driven business economy*, Roma, 2021, 9 ss.

selezione preimpostate, ai vari *dark patterns*[18], oppure agli insidiosi strumenti di *nudging*[19] utilizzati dalle più grandi aziende attive nell'ambito *tech*[20]. Questi attori inoltre rivestono in alcuni casi una posizione dominante[21], come emerge sia dalle sentenze dell'Autorità giudiziaria che dai provvedimenti del Garante della Protezione dei Dati personali[22].
In merito, si consideri l'ordinanza n. 14381 del 2021[23] della Corte di Cassazione in cui il Garante, in un caso riguardante il complesso tema del *social scoring*, ha ritenuto di dover proporre ricorso contro la decisione del Tribunale di Roma, sostenendo che il sistema di *scoring* in esame avesse il potenziale di incidere pesantemente sulla rappresentazione economica e sociale di un'ampia categoria di soggetti, con possibili ripercussioni sul *rating* e sulla vita privata degli individui interessati. Tuttavia, questa posizione del Garante non è stata completamente condivisa dal Tribunale che ha parzialmente accolto il ricorso dell'associazione che utilizzava il sistema di *rating*, annullando la decisione del Garante e ridimensionando dunque il blocco dei trattamenti del servizio. La Cassazione ha accolto il ricorso del Garante, sostenendo che il Tribunale non aveva considerato adeguatamente le garanzie per l'interessato. Nonostante il contesto di trattamenti automatizzati complessi, l'ordinanza ha fatto ricorso al

---

[18] I *dark patterns* sono elementi di interfaccia utente intenzionalmente ingannevoli che mirano ad indirizzare le decisioni degli utenti online verso specifici comportamenti che altrimenti non sarebbero da essi tenuti. L'utilizzo principale, non l'unico, è celare e rendere difficili da trovare le opzioni per rinunciare a determinati servizi o condivisioni di dati per far sì che gli utenti accettino qualcosa senza rendersene conto. Il tema è stato trattato dall'*European Data Protection Board* nelle "*Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*".

[19] Il *nudging* è una teoria nell'ambito dell'economia comportamentale che suggerisce l'utilizzo di rinforzi positivi o l'assenza di rinforzi negativi per influenzare decisioni individuali o di gruppo. Nei contesti delle piattaforme social, il *nudging* si manifesta attraverso strategie di design e presentazione delle opzioni per influenzare il comportamento degli utenti, ad esempio, mediante la spunta preimpostata su caselle di accettazione

[20] G. VERSACI, *Consenso al trattamento dei dati personali e dark patterns tra opzionalità e condizionalità*, in *I problemi dell'informazione nel diritto civile, oggi. Studi in onore di Vincenzo Cuffaro*, a cura di M. D'Auria, Roma, 2022, 463 ss.

[21] N. SEUNGAHN, *Research Handbook on Artificial Intelligence and Communication*, Edward Elgar Publishing, Cheltenham, 2023, 407 ss.

[22] Si pensi, ad esempio, al Provvedimento prescrittivo e sanzionatorio nei confronti di Ediscom S.p.A. - 23 febbraio 2023 [9870014], dove per la prima volta una società, in particolare una società digitale, viene sanzionata per l'utilizzo di *dark pattern*.

[23] Cass., 25.5.2021, n. 14381: la Corte di Cassazione ha emesso un pronunciamento in merito al ricorso presentato dal Garante per la protezione dei dati personali contro la sentenza del Tribunale di Roma concernente il *social scoring*. La Cassazione ha accolto il ricorso, ritenendo che la decisione del Tribunale di Roma non avesse adeguatamente tenuto conto del sistema di garanzie che circonda l'individuo interessato. Nell'ordinanza, pur affrontando trattamenti automatizzati di notevole complessità mediante tecniche algoritmiche, è stato adottato un approccio basato su un concetto tradizionale presente nella normativa sulla protezione dei dati: il consenso dell'interessato come fondamento giuridico del trattamento. La Cassazione ha sottolineato che tale consenso deve essere informato, consentendo all'individuo di comprendere le modalità operative di un trattamento algoritmico in modo da potervi acconsentire liberamente. Infatti, secondo la Cassazione, non è logico presumere che l'adesione a una piattaforma da parte degli utenti implichi automaticamente l'accettazione di un sistema automatizzato basato su un algoritmo per la valutazione oggettiva dei dati personali, a meno che non siano chiaramente resi noti lo schema esecutivo in cui l'algoritmo opera e gli elementi presi in considerazione a tal fine. Nel giudizio di rinvio, il Tribunale di Roma ha respinto il ricorso del titolare, ritenendo che la descrizione dell'algoritmo alla base del sistema di *social scoring* non rispettasse il descritto principio di diritto, in quanto non erano stati spiegati i passaggi logici di calcolo del *rating* finale dell'associato, essenziale per la prestazione di un consenso realmente informato. Sulla base di un ricorso promosso dal titolare, la Corte di Cassazione, con sentenza del 10 ottobre 2023, n. 28358 ha deciso nel merito la causa, annullando il provv. del Garante per la protezione dei dati personali, ritenendo abnorme l'adempimento imposto al titolare di descrivere nel dettaglio l'algoritmo. In tale ordinanza, viene chiarito che per la prestazione di un consenso informato è sufficiente una descrizione di passaggi logici, documentati, prodromici alla determinazione del *rating*, senza scendere in tecnicismi comprensibili solo a un pubblico di "addetti ai lavori".

consenso dell'interessato come base giuridica, sottolineando che deve essere informato e che l'interessato deve conoscere le modalità del trattamento algoritmico.

4. Contestualizzazione dei nuovi orizzonti del consenso nelle dinamiche contemporanee.

Oggi emergono dunque nuovi orizzonti del consenso e nuove sfide con cui occorre confrontarsi.
Un argomento attuale è la possibilità introdotta dal *Data Governance Act* (DGA)[24] di prestare il proprio consenso all'altruismo dei dati, ovvero alla destinazione dei dati a fini solidaristici che il DGA promuove per favorire un utilizzo dei dati personali nell'interesse collettivo come bene comune[25]. Appare chiaro come, in questo caso, il principio di un consenso specifico venga messo in discussione, non potendo l'utente sapere in anticipo ed essere dunque informato circa il trattamento a cui i suoi dati verranno in futuro sottoposti[26].
Medesimo discorso per il trattamento automatizzato dei dati: gli utenti prestano un iniziale consenso a un trattamento che non può essere facilmente perimetrato e la cui spiegazione all'utente risulta particolarmente complessa[27]. Sin dal 2018, i Garanti della protezione dei dati personali del mondo, durante la "*International Conference of Data Protection and Privacy Commissioners – ICDPPC*" dal titolo "*Debating Ethics: Respect and Dignity in Data Driven Life*", hanno approvato la "*Dichiarazione su etica e protezione dei dati nell'intelligenza artificiale*", dove si sono poste le basi di un suo sviluppo ragionato, percependo la difficoltà e le possibili conseguenze derivanti dall'introduzione nella società di tale tecnologia.
Oggi, con l'AI Act[28], il tema è tornato attuale: il consenso qui rappresenta un presidio essenziale di tutela della persona rispetto al rischio di sfruttamento di quei frammenti dell'io che sono appunto i dati personali e di manipolazioni della persona[29].
L'AI Act si preoccupa, poi, di sottrarre anche alla disponibilità del singolo (e dunque al consenso) trattamenti di dati realizzati mediante applicazioni talmente rischiosi in termini democratici (ad esempio, quelli di *social scoring* che ricordano il *social credit system* cinese) da imporre un limite anche all'autonomia privata.
L'utilizzo di tecnologie così affamate di dati, porta alla luce un altro argomento molto discusso: il tema della monetizzazione del dato, ossia dello schema "dati contro servizi". La disponibilità di ingenti quantità di dati personali permette di effettuare analisi accurate circa determinati

---

[24] Reg. (UE) 2022/868 del Parlamento Europeo e del Consiglio del 30.5.2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati).
[25] Con parere congiunto, il Comitato e il Garante europeo per la protezione dei dati personali hanno evidenziato le possibili incongruenze applicative derivanti dai rapporti tra GDPR e proposta di DGA. Tra queste, sono state la necessità di richiamare la nozione di 'consenso' del GDPR, e le interazioni tra il consenso degli interessati e l'altruismo dei dati. Si veda *Parere congiunto EDPB-GEPD 03/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati),* 9 giugno 2021.
[26] A. POGGI e F. FABBRIZI e F. SAVASTANO, *Social network, formazione del consenso e intelligenza artificiale. Itinerario di un percorso di ricerca di Beniamino Caravita,* Roma, 44 ss.
[27] M. BUTTERWORTH, *The ICO and artificial intelligence: the role of fairness in the GDPR framework*, in *34 Computer Law & Security Review*, 2018, 257 ss.
[28] Reg. (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13.6.2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).
[29] Per un approfondimento sul tema, M. R. LEISER, *Psychological Patterns and Article 5 of the AI Act: AI-Powered Deceptive Design in the System Architecture and the User Interface*, in *Journal of AI law and Regulation*, 2023, 5 ss.

cluster che si intendono studiare. Per questo motivo, le aziende nel tempo hanno cercato di carpire il più possibile tali dati dai propri utenti. In primo luogo, se da un lato non occorre demonizzare tale pratica, in quanto portatrice anche di indubbi vantaggi per la persona, come per esempio servizi *tailor-made*; d'altra parte, è indubbio che essa metta, almeno apparentemente, in discussione l'architettura *privacy* fino ad ora raccontata.

5. Consenso: un'evoluzione del concetto di consenso e coesistenza con pratiche negoziali sul dato personale.

Se il consenso *privacy* diventa autorizzazione ad una controprestazione commerciale, di scambio di cosa contro prezzo, o di dato in questo caso, è possibile che esso sia stato svuotato del suo significato?
In realtà non si ritiene debba essere così. Posto che le nascenti tecnologie offriranno sempre più nodi cruciali da sciogliere, il consenso *privacy* è strumentale all'esercizio di un diritto fondamentale del cittadino, quello alla protezione dei dati personali, ma occorre adattarlo e renderlo effettivo. La dottrina e la giurisprudenza naturalmente sottolineano l'importanza che ciò non si traduca in potenziali forme di danno alla persona e di mercificazione dell'identità personale degli interessati.
L'impatto dell'innovazione ed il progressivo spostamento dell'asse della propria vita dal mondo reale a quello virtuale contribuiscono all'evoluzione del principio consensualistico da mero presupposto di liceità del trattamento a strumento di controllo sui propri flussi informativi ed elemento di conformazione e costruzione della propria sfera privata[30]. Per questo motivo diventerà sempre più essenziale garantire sin dal principio che tecnologie che operino un ingente trattamento di dati non siano concepite in modo da sfruttare le vulnerabilità degli interessati.

[30] A. VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale*, Napoli, 2019.

LIBERTÀ E LICEITÀ DEL CONSENSO NEL TRATTAMENTO DEI DATI. UNA PREMESSA

Di Giuseppe Vettori

SOMMARIO*: *1. Le regole. – 2. La libertà il consenso e la categoria del dovere. – 3. I rimedi e il loro cumulo.- 4. La Persona come frutto di un'azione ordinante.

1. Le regole.

La rivoluzione digitale sta trasformando la nostra vita e la tecnologia, sempre più potente, si evolve con una velocità straordinaria. Si parla di un nuovo ordine del tempo con tratti del tutto peculiari perché il trattamento dei dati è divenuto una forma di dominio dove non si usa apparentemente violenza, perché il soggetto sottomesso si crede libero e creativo e spesso non avverte la gravità delle distorsioni[1]. Non solo.
L'ordine digitale abolisce la solidità dei fatti, produce una nuova realtà virtuale, disperde la stabilità dell'essere in una Info-crazia dominata appunto dal potere digitale. Certo, i filosofi più attenti e autorevoli ci ricordano che la "scissione demonizzata fra l'uomo e la tecnica è inutile perché quanto più l'uomo avverte la tecnica estranea a sé, tanto più quella gli restituisce la sua stessa immagine umana". Perché l'intelligenza artificiale è espressione di quello stesso *logos* che si immagina all'opera nell'atto della lettura, del dialogo con i propri simili, nella contemplazione dell'Universo[2]. Dunque, tutto ciò richiede al civilista in particolare un'ermeneutica idonea a comprendere il nuovo e una nuova teoria capace di costruire garanzie e tutele adatte ai tempi. Senza la tentazione del disincanto, inutile e pericolosa. Per una ragione chiara.
Siamo in presenza di una ennesima transizione dove gli apparati tecnici generano nuove forme dell'umano e una nuova oggettività giuridica ancora in gran parte da costruire. Sappiamo ancora poco. Certo è che telematica e robotica producono conoscenza, non hanno limiti spaziali e consentono un enorme accumulo di potere in mano a pochi.
Da qui la necessità di riflettere sulla regolazione privata e pubblica in Europa.
A ben vedere già il Regolamento Generale sulla Protezione dei Dati Personali (GDPR) si basava su un'indicazione primaria. La profilazione e la previsione automatica di comportamenti futuri non deve essere utilizzata nelle decisioni relative a qualsiasi soggetto in una società che riconosca i diritti fondamentali di ogni Persona. Il perché è chiaro. La raccolta di dati crea categorie e classificazioni sempre a rischio di discriminazioni e di decisioni imprecise e spesso irrazionali. Ciò che avvenuto dopo è noto[3].

---

[1] B. CHUL HAN, *Infocrazia. Le nostre vite manipolate dalla rete*., Torino, 2021, 8 ss.
[2] A. PUNZI, *La persona del futuro. Il dialogo delle intelligenze tra umanesimo e tecnoscienze*, in *Pers. merc.*, 2023, 161 ss.
[3] S. ORLANDO, *Consenso al trattamento e liceità*, in *Pers. merc.*, 2024, 333 ss.; ID., *Regole di immissione sul mercato e "pratiche di intelligenza artificiale" vietate nella proposta di Artificial intelligence act*, in *Pers. merc.*, 2022, 346 ss.; ID., *Per un sindacato di liceità del consenso privacy*, in *Pers. merc.*, 2022, 527 ss.; V. RICCIUTO, *Il*

Il regolamento DSA è entrato in vigore il 16 novembre 2022. L'UE ha iniziato ad applicarlo individuando 17 piattaforme e 2 motori di ricerca che devono adeguarsi alla disciplina comunitaria sulla base di informazioni chiare, e soprattutto di un dovere di progettare i loro sistemi per garantire un elevato livello di tutela della vita privata e in particolare dei minori. Le piattaforme dovranno garantire il rispetto del Regolamento e saranno sottoposte alla vigilanza di un audit esterno e indipendente. È stato costituito un centro europeo per la trasparenza algoritmica (ECAT) che fornirà alla commissione competenze tecniche e scientifiche per assicurare che i sistemi (algoritmici) delle piattaforme rispettino i requisiti del DSA e per controllare "l'impatto sociale a lungo termine della loro attività".
Come è noto il Garante italiano ha sospeso l'attività della Chat GPT e sollevato per primo il problema di una tutela dei diritti fondamentali degli utenti. Le misure richieste riguardavano in particolare il c.d. addestramento degli algoritmi della Chat GPT tramite la profilazione degli utenti e l'età dei fruitori. Dopo tale intervento, OpenAI ha previsto una procedura per consentire di disabilitare l'addestramento, l'esclusione dal servizio dei minori di 13 anni e un uso 'assistito' per i minori fra 13 e 17 anni. Si è così riattivato il servizio, anche se il Garante ha dichiarato che proseguirà nella sua istruttoria in accordo con le altre Autorità europee.
Non solo.
Il Garante europeo ha formulato un parere sull'AI Act. Ha indicato la necessità di vietare sistemi che operano sul riconoscimento automatico di caratteristiche umane, di rimuovere le forme di profilazione ad alto rischio, e di attribuire alle Autorità Garanti la competenza a ricevere reclami. Si accoglie con favore l'Istituzione di un Ufficio europeo per l'IA e la possibilità di svolgere indagini in collaborazione con le Autorità nazionali. In un quadro plurale di organi e Istituzioni di Vigilanza e di controllo a cui si aggiunge il ruolo importante della CGUE (sul recente caso dell'equo compenso).
Siamo in presenza insomma di una nuova stagione regolatoria[4], che si rivolge ad una pluralità di attori e di fonti. Dalla disciplina consumeristica sulle pratiche scorrette[5] a nuovi strumenti privatistici[6], ove "assume speciale rilievo la clausola generale della diligenza professionale" e con essa "l'insieme dei doveri di cura e attenzione incombenti sul professionista, desumibili tenendo conto della natura della pratica, del settore e tipo di prodotto o servizio, nonché del consumatore medio destinatario della stessa". Con una consapevolezza. L'insufficienza della nozione di autonomia negoziale, contenuta nel codice civile e la necessità di nuove forme di tutela della libertà del singolo[7]. Solo un esempio.
Nel giro di pochi mesi, l'Unione Europea ha emanato Regole e Principi sul consenso nel mondo digitale. Si disciplina la sua distorsione, la sua molteplice rilevanza, e il diverso ruolo del

---

contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali, in *Riv. dir. civ.*, 2020, 642 ss. e 652 ss.; G. FINOCCHIARO, *Intelligenza artificiale. Quali regole?,* Bologna, 40 ss.

[4] S. ORLANDO, *Consenso al trattamento e liceità*, cit.; R. MONTINARO, *I sistemi di raccomandazione sulle interazioni tra professionisti e consumatori: il punto di vista del diritto dei consumi (e non solo),* in *Pers. merc.*, 2022, 368 ss.

[5] R. MONTINARO, *op. cit.*, p. 390 e il riferimento alla riforma "Secondo le Linee guida Commissione UE 2021, par. 4.2.7., «Le pratiche di personalizzazione basate sui dati nel rapporto tra impresa e consumatore comprendono la personalizza zione della pubblicità, sistemi di raccomandazione, la tariffazione, la classificazione delle offerte nei risultati di ricerca, ecc. Le norme e i divieti di principio contenuti nella direttiva possono essere utilizzati per contrastare le pratiche commerciali sleali delle imprese nei confronti dei consumatori oltre ad altri strumenti del quadro giuridico dell'UE, come la direttiva relativa alla vita privata e alle comunicazioni elettroniche, il GDPR oppure la legislazione settoriale applicabile alle piattaforme online»".

[6] R. MONTINARO, *op. ult. cit.*, nota 152: "Ivi inclusi quelli di natura collettiva di cui alla direttiva 2020/1828/UE del Parlamento e del Consiglio del 25 novembre 2020 relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE (L 409/1), la quale si ripropone di governare i due fenomeni della globalizzazione e della digitalizzazione offrendo tutele improntate al principio di effettività e concernenti gli interessi collettivi (cfr. Considerando 1 e 7)".

[7] R. MONTINARO, *op. cit.*, nota 159 e il rinvio a N. IRTI, *Letture bettiane sul negozio giuridico*, Milano 1991.

controllo. Un sistema ordinato era già emerso nella Direttiva sulle pratiche commerciali scorrette (2005/29/CE) e si completa ora con l'AI Act. Non si vieta l'orientamento ma la distorsione delle decisioni mediante due proibizioni: falsare la decisione e approfittare di condizioni soggettive di media vulnerabilità. Il carattere innovativo sta nel descrivere precise condizioni di fragilità. In un elenco si parla di ignoranza, disattenzione, sprovvedutezza, impressionabilità, incapacità di resistenza (psichica o economica), di incapacità (psichica o economica) di reazione. Oltre a disciplinare le pratiche aggressive che intaccano il tema della libertà. Ne segue, da un lato un divieto di distorcere il consenso e di approfittare delle condizioni di debolezza, dall'altro il dovere di comportarsi secondo la diligenza professionale. Che cosa cambia nel sistema privatistico dei rimedi è chiaro.
Se il tema della correttezza e della buona fede è la base comune di valutazione, il legislatore europeo muta la tecnica dei codici. Dal divieto generale alle fattispecie tipiche ingannevoli e aggressive ai Regolamenti successivi che introducono una rilevanza plurima alla distorsione del consenso. Dagli artt. 25, 26, 27 DSA all'art. 5, lett. a e d AI Act. Non si tratta di un complesso di regole caotico e diffuso ma di un sistema che segue linee precise di disciplina, del prodotto e dell'attività del professionista, delle tutele pubbliche e private. Secondo una multipolarità e uno scenario multilivello, che esigono un pensiero forte e creativo[8]. Nel ripensare le tutele invalidanti e risarcitorie e il loro possibile cumulo, come vedremo.
Alcune precisazioni sono oramai patrimonio comune grazie a lucide e profonde analisi [9]. Spetta ora alla Scienza Giuridica elaborare una nuova dogmatica spinta da precise norme. Solo qualche esempio.

2. La libertà il consenso e la categoria del dovere.

Sempre più spesso "il contratto sprigiona i suoi effetti vincolanti, ma la mitologia della voluntas nasconde un enorme vuoto"; al di là del "monumentale edificio del contratto (…) frutto dell'operosità di una generazioni di giuristi infaticabili": ciò che si intravede in molti 'accordi' è "*il nulla*"; Sempre più "viene in evidenza una dialettica fra un fuori che è visibile e governa, e un dentro, che non c'è"[10].
La vincolatività del contratto determinata dalla volontà di chi lo conclude è un solo una finzione. Da qui la necessità[11] di un nuovo ruolo del diritto civile. Sulla base di una premessa. "Non c'è una sola verità giuridica, la quale ha la sua fonte nella legge e viene fedelmente ricostruita dalla dottrina e applicata dalla giurisprudenza"[12]. Occorrono regole nuove. Ma non solo. Sono necessarie, come sempre, costruzioni teoriche che, per l'autorità di chi le ha formulate, e per la loro capacità persuasiva[13] possano acquisire un valore ordinante. Basta un esempio.
Il consenso nel mondo digitale e la tutela contro le piattaforme e i poteri privati è un tema attualissimo[14]. Le Corti nazionali e la Corte di Giustizia sono impegnate in due delicate

---

[8] S. ORLANDO, *Consenso al trattamento e liceità*, cit.; G. FINOCCHIARO, *Intelligenza artificiale. Quali regole?*, cit.; D. IMBRUGLIA, *La presunzione delle macchine e il consenso dell'interessato*, in *Riv. trim. dir. proc. civ.*, 2023, 921 ss.
[9] F. RENDE, Abus de dépendance *e controllo del regolamento contrattuale,* in *Liber amicorum per Giuseppe Vettori*, a cura di G. Passagnoli, F. Addis, G. Capaldo, A. Rizzi e S. Orlando, Firenze, 2022, 3599 ss.
[10] T. DALLA MASSARA, *Il consenso annichilito*, Bologna, 2021, 133 ss. e il richiamo a R. ESPOSITO, *Da fuori. Una filosofia per l'Europa*, Torino, 2016.
[11] T. DALLA MASSARA, *op. ult. cit.*, 139-140.
[12] R. SACCO, *Introduzione al diritto comparato*, ora in *Trattato di diritto comparato*, diretto da R. Sacco, Torino, 2009, 16 ss.
[13] R. SACCO, *op. ult. cit.*, 46 e 77.
[14] R. PARDOLESI, *Piattaforme digitali, poteri privati e concorrenza*, in *Dir. pubblico*, 2022, 941 ss.

operazioni: a) assicurare la più intensa effettività delle tutele con una sinergia forte fra Regole e Principi di diversa provenienza[15]; b) potenziare le situazioni soggettive anche attraverso forme di tutela collettiva per diritti individuali omogenei o interessi superindividuali verso un bene da proteggere in modo nuovo e diverso dal passato[16]. Di più.
Le nuove regole sull'intelligenza artificiale sono oggetto di grande attenzione da parte dei civilisti[17]. Impegnati a chiarire gli obbiettivi della regolazione e la disciplina di un contratto che è tale "anche se concluso da un sistema di IA". Il che implica prestare attenzione ad enti, come l'UNCITRAL, impegnati nel ripensare "le dichiarazione di volontà, [i] vizi del consenso, [i] doveri di informazione precontrattuale, [la] tracciabilità, [la] responsabilità e [l'] esecuzione automatica del contratto". Ma non solo. Si dovranno applicare e rivedere le norme vigenti e tener conto dei Principi che da ultimo (art. 4 *bis* AI Act) orientano in modo molto dettagliato e con un "approccio fondamentalmente regolatorio", molto diverso da di quanto avviene negli Stati uniti, ove si è scelto , ancora una volta, "un percorso condiviso con il mercato"[18].
Molti problemi riguardano la riflessione sui dati e sul ruolo dell'autonomia privata e del consenso al loro trattamento[19] con una riflessione iniziata in Italia di fronte ad un panorama normativo esteso. Si ricorda come solo nel 2022 si sono elencate ben 48 normative, emanate o allo studio, in oltre 30 anni e posto in luce l'esigenza di una sistemazione organica [20] di tre gruppi di discipline: in primo luogo la direttiva privacy del 1995 abrogata dal GDPR del 2016 e poi il DSA, il DMA e ora l'AI Act[21].

3. I rimedi e il loro cumulo.

Per quanto attiene ai rimedi privatistici è evidente l'esigenza di ripensare le nostre categorie ordinanti per una pluralità di motivi.

---

[15] La CGUE è favorevole all'utilizzo dei rimedi previsti dalla disciplina del consumo per garantire il rispetto della normativa sulla privacy prevista dal GDPR del 2016 instaurando una sinergia forte fra e protezione dei dati. Basta esaminare le conclusioni dell'avvocato generale in Meta-Bundesvezband, 319/20 C.2021/979 e la decisione CGUE 28.4.2022, C-319/20. Si veda anche M. FEDERICO, *Rappresentanza degli interessati, diritti individuali e group data protection*, in *Pers. Merc*., 2022, 674 ss. e le conclusioni dell'avvocato A. Rantos del 20.9.2022 nella causa C252/21 fra Meta e Bundeskartellamt.
[16] A. PUNZI, *op. cit.*, 183-184 e il richiamo a M. FERRARIS, *Documanità. Filosofia del mondo nuovo*, Bari-Roma, 2021, 333 e 338.
[17] Da ultimo, G. FINOCCHIARO, *op. cit.*, 40 ss. e, come riferimento generale, N. BOBBIO, *Libertà*, in *Enciclopedia del Novecento*, III, Milano-Roma, 1978, 1003.
[18] Cosi in modo molto efficace, G. FINOCCHIARO, *op. cit.*, p. 42-48.
[19] V. RICCIUTO, *op. cit.*, 642 ss., spec. p. 652; ID., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio e V. Ricciuto, Torino, 2019, 29; ID., *L'equivoco della privacy. Persona vs dato personale*, Napoli, 2022 (su cui v. anche le recensioni di G. CARAPEZZA FIGLIA, *"L'equivoco della privacy". Circolazione dei dati personali e tutela della persona*, in *Jus Civile*, 2022, 1372 ss. e di R. SENIGAGLIA, *"L'equivoco della privacy" tra consenso e capacità*, in *Jus Civile*, p. 1378 ss.); S. ORLANDO, *Data vs Capta: intorno alla definizione dei dati*, in *Nuovo Dir. Civ.*, 2022, 14 ss. ed ivi un amplissima analisi della dottrina degli ultimi anni e dell'evoluzione dei dati normativi e giurisprudenziali. In particolare il riferimento a *Il ruolo del Garante per la protezione dei dati personali: la tutela di un diritto fondamentale tra sfide passate e scommesse per il futuro*, a cura di P. Stanzione, i cui atti sono in corso di pubblicazione per i tipi de il Mulino; A. ASTONE, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle* cose, Milano, 2019; ID., *L'accesso dei minori di età ai servizi della c.d. società* dell'informazione, in *Contr. impr.*, 2019, 614
[20] S. ORLANDO, *Data vs capta*, cit. e il richiamo alla Comunicazione della Commissione "*Una strategia europea per i dati*" (COM/2020/66 final del 19 febbraio 2020), nonché a: D. POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy Law and technologies*, 2022, 46 ss.; G. CAPALDO, *La strategia digitale dell'Unione Europea verso un mercato unico sostenibile*, in *Annuario 2021 Osservatorio Giuridico sull'Innovazione Digitale*, a cura di S. Orlando e G. Capaldo, Roma, 2021, 35 ss.
[21] S. ORLANDO, *op. loc. ult. cit.*

La circolazione dei dati non è riducibile al modello della *privacy* né al paradigma proprietario degli atti di scambio. Il trattamento è disciplinato in buona parte anche dal diritto delle obbligazioni e del contratto e ciò implica un concorso e un'interazione di tutele perché a seconda del contesto nei quali agisce la Persona è ora contraente ora imprenditore, ora consumatore e dunque soggetto a diversi modelli rimediali.
Dunque, si dovranno considerare le limitazioni legali relative alla natura del bene, la liceità del trattamento (art. 6 GDPR), la possibile revoca del consenso (art. 7 GDPR) e i diritti dell'interessato (15-20 GDPR). Sulla base di una precisa indicazione. Non esiste un diritto unico alla personalità a contenuto indefinito o uno statuto unico della Persona, come sembra presupporre sin dal titolo la Direttiva 95/46/CEE e la legge italiana sulla *privacy* del 1996. Né si può individuare, in presenza di una lesione, un'unica situazione soggettiva. D'altra parte non sempre è utile il riconoscimento esplicito di un diritto, perché il divieto e il dovere sono spesso più adatti alla protezione della libertà e dell'autonomia dei privati. Mentre le Autorità Garanti debbono poter disporre di poteri sanzionatori e inibitori. La lettura sistematica della c.d. Direttiva omnibus del 2 aprile 2023 può consentire all'AGCM di inibire l'utilizzo e l'uso di clausole vessatorie come pratica commerciale ingannevole. La lettura in tal senso degli articoli 27 e 37 *bis* del Codice del Consumo è condivisibile[22].
Certo è che la nuova regolazione ci pone di fronte ad un dato evidente in Italia. Da un lato, la insufficienza della teoria generale dei diritti della persona e del contratto contenuta nel Codice Civile. Dall'altro un enorme produzione di regole, per lo più, di derivazione europea che richiede un metodo e un'attività precisa. Assumere il contratto e l'illecito "*come termini alternativi per una valutazione delle situazioni soggettive tutelate*", è un errore perché si vede solo metà del fenomeno e non si colgono "*tutti i profili valutativi in ordine alla precisazione di un limite alla condotta che può derivare dalla presenza di un contratto*"[23]. Sul punto la dogmatica ci è di aiuto in modo decisivo.
Ogni "*figura di qualificazione giuridica si esaurisce logicamente in sé e non ha l'efficienza di dar luogo automaticamente a nuove conseguenze giuridiche*" e così nel contratto non è dato trovare gli elementi per risolvere un problema di sistemazione che è ad esso estraneo. Può accadere che una preesistente qualificazione giuridica di un atto sia la base per il sorgere di nuove conseguenze, ma in tal caso quel elemento di ordine formale precipita ad elemento di fatto. Ed è ciò che avviene nel nostro caso. "*Nella valutazione delle interferenze e dei limiti alla condotta che si verificano per la presenza di un contratto questo non è che una situazione-presupposto per il sorgere di nuove ed eventuali conseguenze giuridiche, per la cui realizzazione entrano in gioco altre norme che assumono come elementi di fatto, appunto, la fattispecie e i contegni che in concreto determinano il verificarsi delle interferenze*"[24]. Se ciò è esatto la conseguenza che può trarsi è questa.
"*Ogni assetto di interessi privato va esaminato come atto, in base ad una valutazione strutturale di validità e come insieme dei contegni formativi ed esecutivi in base ad una valutazione dinamica che può condurre ad una pronunzia di responsabilità. Perché la disciplina dell'atto e dei contegni è diversa, come autonome e cumulabili sono le due valutazioni di validità e di responsabilità*»[25]. Questa conclusione era già stata affermata dalla Corte di Cassazione e ribadita con estrema lucidità e con profili del tutto innovativi, condivisi

[22] S. ORLANDO, *Consenso al trattamento e liceità*, cit.
[23] Richiamo qui alcune considerazione contenute in G. VETTORI, *Validità, responsabilità e cumulo dei rimedi. A proposito del caso Cir-Fininvest,* in *Pers. merc.*, 2016, 279 ss.
[24] A.E. CAMMARATA, *Limiti fra formalismo e dommatica nelle figure di qualificazione giuridica*, in *Formalismo e sapere giuridico. Studi*, Milano, 1963, 390 ss., spec. 391.
[25] G. VETTORI, *Efficacia e opponibilità del patto di preferenza*, Roma, 1988, 144. Mi permetto di rinviare solo per una sintesi delle varie opinioni a G. VETTORI, *Diritto privato e ordinamento comunitario*, Milano, 2009, 252 ss. e 271 ss.

da una parte della dottrina[26]. La risarcibilità del c.d. 'danno da scorrettezza' in "funzione correttiva dell'equilibrio economico risultante dal contratto" è stato ritenuto "compatibile con il principio di certezza e stabilità dei fatti giuridici" perché validità e responsabilità "operano su piani diversi e non possono entrare in contraddizione". Tale azione valuta un comportamento e il giudizio non incide sul controllo strutturale dell'atto di autonomia, ma corregge, sul piano risarcitorio, il contenuto del contratto secondo quanto è riconosciuto da una pluralità di fonti[27].

4. La Persona come frutto di un'azione ordinante.

Se i confini fra naturale e artificiale sembrano confondersi si deve usare un concetto di Persona diverso dal passato. Non un'idea ontologica ma il frutto di un'azione ordinante da svolgere giorno per giorno. Occorre chiedersi cosa significhi "essere Persona in un mondo sempre più abitato da entità non umane ma pensanti e parlanti". Sulla base di un nuovo sapere e di una nuova cultura che sappia andare oltre la mera separazione fra scienze dure e pensiero umanistico. Si deve attenuare la dicotomia naturale/artificiale e ritrovare nell'artificio l'espressione della nostra "natura inventiva, fra Galileo a Leonardo"[28].
Il che porta a riconoscere che la Persona non è un'entità astratta, fuori dal tempo, ma vive nel tempo e lo condiziona, in base a nuovi 'istituti della libertà', a plurime tutele e garanzie della sua autonomia, e indipendenza. Dunque non una forma intangibile ma una sintesi, diversa nel tempo, di diritti, doveri, tutele che appartengono al diritto e alla morale ma devono essere attuati con strumenti e procedure del diritto sulla base di un'"oggettività ideale e giuridica" espressa

[26] Così, M. MANTOVANI, *Vizi incompleti del contratto e rimedio risarcitorio*, Torino, 1995 e già: F. BENATTI, *Culpa in contraendo*, 1987, 298; G. VETTORI, *Anomalie e tutele nei contratti di distribuzione fra imprese. Diritto dei contratti e regole di concorrenza*, Milano, 1983, 68 ss.
[27] Uno sguardo ai Principi e alla giurisprudenza comunitaria conferma il quadro che sopra si è ricostruito per la disciplina interna. Basta un rapido cenno alla soft law e non solo. L'art. 8.102 dei PECL (Principi di diritto europeo dei contratti) e l'art. 3.102 (*cumulation of remedies)* del Charter 3 del DCFR affermano la possibilità di un cumulo dei rimedi con il solo limite della compatibilità. Gli artt. 7:216 e 7:304 del Charter 7 del DCFR prevedono la possibilità di altri rimedi in presenza di un'invalidità. La Convenzione sulla vendita internazionale di merci agli art. 45 (obblighi del venditore) e 61 (obblighi dell'acquirente) prevedono la possibilità di cumulo fra adempimento, risoluzione e risarcimento. La Proposta di Regolamento relativo ad un diritto co-mune europeo della vendita, all'art. 29 (Rimedi in caso di violazione di un obbligo di informazione) prevede che il risarcimento non pregiudica l'applicazione dei rimedi previsti nell'art. 42 (recesso), 48 (dolo) e negli altri casi di annullamento o inefficacia del contratto. La sentenza *Courage* della Corte di Giustizia afferma la compatibilità fra un'azione di danni del consumatore pur in presenza di una nullità del con-tratto a cui lui stesso ha dato causa. Alla Corte era stato richiesto se osta con il diritto comunitario «il risarcimento di un preteso danno subito a causa dell'assoggettamento della parte ad una clausola contrattuale, in contrasto con l'art. 85 e, di conseguenza, se il diritto comunitario osti ad una norma di diritto nazionale che nega ad un soggetto il diritto di fondarsi sui propri atti illeciti per ottenere un risarcimento dei danni». La risposta è stata netta. «Qualsiasi singolo è legittimato a far valere in giudizio la violazione dell'art. 85 n. 1 del Trattato, anche qualora sia parte di un contratto che può re-stringere o falsare il gioco della concorrenza ai sensi di tale disposizione». «La piena efficacia dell'art. 85 del Trattato e l'effetto utile del divieto sancito al n. 1 di detto articolo sarebbero messi in discussione se fosse impossibile per chiunque chiedere il risarcimento del danno causatogli da un contratto o da un comportamento idoneo a restringere o falsare il gioco della concorrenza». Ancora. Dagli artt. 3 e 24 della Costituzione si evince, con un sillogismo chiaro, il principio di effettività della tutela a fronte di diritti e interessi meritevoli. «Il titolare del diritto deve (poter contare) su mezzi che gli consentano di reagire alla violazione», e di reazione si può parlare solo là dove vi è proporzione tra tutela e offesa arrecata. Sicché non è in armonia con l'art. 24 una tutela che si esprime in un risarcimento non pari al danno cagionato o al sacrificio subito. L'art. 8 della Dichiarazione Universale dei diritti dell'uomo, l'art. 13 della Convenzione europea dei diritti dell'uomo e l'art. 47 della Carta dei diritti fondamentali dell'Unione europea esprimono tutti un principio che si manifesta, non solo come «un diritto di accesso al giudizio o all'esercizio in esso di un determinato potere processuale», ma come «diritto alla misura appropriata alla soddisfazione del bisogno di tutela».
[28] A. PUNZI, *op. cit*.

nei documenti europei[29]. Con una premessa assoluta. Il pluralismo, giuridico, politico e sociale e la difesa della Persona sono una coppia teorica e operativa intangibile e inseparabile. Fonte di un'attività creativa dell'interprete per ripensare e ampliare le tutele e i rimedi individuali e collettivi.

[29] L. MENGONI, *Diritto e tecnica*, in *Riv. trim. dir. proc. civ.*, 2001, 7.

CONSENSO AL TRATTAMENTO E LIBERTÀ

Di Giusella Finocchiaro

SOMMARIO: 1. Introduzione. Consenso e libertà nel contratto e nel trattamento dei dati personali. - 2. Il quadro normativo. - 3. Gli orientamenti giurisprudenziali. - 4. La libertà del consenso in una dimensione contestuale.

1. Introduzione. Consenso e libertà nel contratto e nel trattamento dei dati personali.

Consenso e libertà si declinano oggi anche in due ambiti che appaiono essere sempre più prossimi: quello del contratto e quello del trattamento dei dati personali. Se, infatti, fino a qualche tempo fa la cesura fra patrimonialità e non patrimonialità era netta, ora essa non è più così evidente.
È noto che per molto tempo la riflessione sul consenso (e quindi sulla libertà dello stesso) nel contratto e quella sul consenso (e, quindi, sulla libertà del medesimo) nel trattamento dei dati personali abbiano proceduto lungo due binari differenti e paralleli, che si assumeva fossero destinati a non incontrarsi: da un lato quello del contratto e dei diritti patrimoniali, e dall'altro quello dei diritti della persona e dei diritti non patrimoniali e indisponibili. Ora i due binari non paiono più inevitabilmente paralleli ma si intrecciano, in modi non del tutto scontati.
Il discorso sulla libertà, oggetto di questo scritto, si svolge in entrambi gli ambiti individuati: per un verso, l'ambito della libertà negoziale, di tipo contrattuale e, per un altro, l'ambito della libertà nella protezione dei dati personali. Nell'ambito contrattuale, poi, si può praticare un'ulteriore specificazione, che attiene ai contratti con i consumatori.
La libertà riguarda la fase di formazione della volontà e la fase di espressione della medesima: è dunque libertà *di* e *nell'*esprimere il consenso. Acquisite le informazioni necessarie, la volontà è libera nella formazione e poi, in assenza di coercizioni, anche di tipo tecnologico, nella sua espressione.
Sotto il profilo normativo, quindi, occorre considerare le disposizioni in materia di contratto in generale, quelle in materia di contratti con i consumatori e poi quelle concernenti il trattamento dei dati personali.

2. Il quadro normativo.

Il tema in oggetto trova il suo più diretto referente normativo nel combinato disposto dell'art. 4, n. 11, e dell'art. 7 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati", ormai più noto come "GDPR", che detta i requisiti di validità del consenso, quale base giuridica del trattamento (art. 6, 1° co., lett. a)[1].

[1] Si segnala, al riguardo, l'interessante posizione di S. ORLANDO, *Per un sindacato di liceità del consenso privacy*, in *Pers. merc.*, 2022, 536 ss.

Secondo l'art. 4, n. 11, per "consenso dell'interessato" s'intende "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento".
L'art. 7, invece, al 1° co., precisa che "qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali". E poi, al 4° co., che: "nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto".
Il 4° co. dell'art. 7 GDPR – che si occupa della condizionalità, o "conditionality" del consenso dell'interessato – rappresenta la prima e, in una prospettiva interna alla *data protection*, la principale disposizione da considerare per la soluzione del quesito se la libertà dell'interessato possa coesistere con la logica dello "scambio" e della remunerazione del consenso al trattamento[2]. Si utilizza qui il termine "scambio" in senso economico e non giuridico, e quindi atecnico, senza volersi in alcun modo riferire al tipo di contratto che eventualmente disciplinerebbe tale scambio, tema che non è oggetto di questo scritto.
In ambito contrattuale, le disposizioni che integrano il quadro normativo si leggono nel Codice del Consumo[3] e, in particolare, nelle recentissime modifiche apportate dal legislatore italiano chiamato ad attuare le due direttive europee in materia.
Giova considerare, in particolare, le seguenti disposizioni.
Innanzitutto, l'art. 3, 1° co., secondo periodo, della 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", che recita: "la presente direttiva si applica altresì nel caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dall'operatore economico ai fini della fornitura del contenuto digitale o del servizio digitale a norma della presente direttiva o per consentire l'assolvimento degli obblighi di legge cui è soggetto l'operatore economico e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti"[4].
E inoltre, l'art. 4, n. 2, lett. b), della Direttiva (UE) 2019/2161 del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori, c.d. "Direttiva Omnibus", ove si legge: "la presente direttiva si applica anche se il professionista fornisce o si impegna a fornire un contenuto digitale mediante un supporto non materiale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali al professionista, tranne i casi in cui i dati personali forniti dal consumatore siano trattati dal professionista esclusivamente ai fini della fornitura del contenuto digitale su supporto non materiale o del servizio digitale a norma della presente direttiva o per consentire l'assolvimento degli obblighi di legge cui il professionista è soggetto, e questi non tratti tali dati per nessun altro scopo"[5].

---

[2] Sull'interpretazione della norma v. le Linee Guida dello EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 05/2020 on consent under Regulation 2016/679*, 4.5.2020, § 25 ss.
[3] Si tratta, come è noto, del D.Lg. 6.9.2005, n. 206.
[4] Disposizione quasi letteralmente ripresa nel recepimento italiano, dall'art. 135 *octies* Cod. cons. modificato dal d.lgs. 4.11.2021, n. 173.
[5] Disposizione quasi letteralmente ripresa nel recepimento italiano, dal nuovo co. 1 *bis* dell'art. 46 Cod. cons., modificato dal d.lg. 7.3.2023, n. 26.

Tale estensione delle tutele consumeristiche conferma che, almeno in via di principio, l'interessato può esercitare la propria libertà di prestare il consenso anche allo scopo di usufruire di contenuti e di servizi, in luogo di pagarne il prezzo in denaro, benché le norme citate individuino un rapporto di contestualità e non di causalità.
La disposizione dell'art. 7 si presta ad essere intesa, sostanzialmente, secondo due chiavi di lettura.
Secondo un approccio più tradizionale, già la sola dimensione dello 'scambio' basta a condizionare irrimediabilmente la libertà dell'interessato. Si ritiene che laddove vi sia un contratto non vi possa essere libertà del consenso al trattamento dei dati: il fatto che il godimento di un bene o la fruizione di un servizio rappresentino la contropartita della fornitura delle informazioni relative alla persona fisica renderebbe il consenso al loro sfruttamento senz'altro necessitato[6].
Secondo una diversa impostazione, che intende coniugare commerciabilità dei dati personali e protezione della persona, l'idea dello 'scambio' appare in astratto compatibile con la libertà del consenso. In questa prospettiva, l'art. 7, 4° co., GDPR rappresenta il riconoscimento, e non già la negazione, della possibilità di esercitare la libertà di determinazione informativa ottenendo una remunerazione per il consenso al trattamento[7].

3. Gli orientamenti giurisprudenziali.

Il tema della libertà del consenso al trattamento, con particolare riguardo allo 'scambio' di dati personali per la fruizione di servizi *on line*, è stato oggetto di crescente attenzione, negli ultimi anni, da parte della giurisprudenza[8].

---

[6] Sul punto, v. A. GENTILI, *La volontà nel contesto digitale: interessi del mercato e diritti delle persone*, in *Riv., trim. dir. proc. civ.*, 2022, 711 ss.: "In linea di principio sono dunque illegittime le operazioni di tying, cioè di offerta di una prestazione subordinatamente al consenso al trattamento per finalità non necessarie". L'Autore richiama una risalente posizione del Garante italiano, il quale nel provvedimento inibitorio e prescrittivo nei confronti di AdSpray S.r.l. del 25 settembre 2014 rilevava: "come già più volte rilevato da questa Autorità (…) non può definirsi 'libero', e risulta indebitamente necessitato, il consenso a ulteriori trattamenti di dati personali che l'interessato debba prestare quale condizione per conseguire una prestazione richiesta" (provv. n. 427 del 25 settembre 2014, doc. *web* n. 3457687). Si occupano del tema anche G. RESTA e V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, 411 ss.

[7] Sintetizza il punto C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, 96: "Subordinare l'esecuzione di un contratto alla prestazione del consenso al trattamento dei dati è circostanza da tenere 'nella massima considerazione' ai fini di valutare la libertà del consenso senza che, tuttavia, dalla norma possa trarsi un divieto generalizzato di porre in essere uno scambio tra la prestazione di un servizio e il rilascio del consenso al trattamento dei dati per finalità estranee all'esecuzione di quel servizio".

[8] La questione è stata analizzata approfonditamente anche dalla dottrina. La dottrina più recente tende ad ammettere che la libertà dell'interessato possa declinarsi anche nella direzione dello "scambio" dei dati personali contro contenuti e servizi digitali, sottolineando, però, che il requisito della libertà dell'interessato va inteso in senso rigoroso. Naturalmente, le ipotesi ricostruttive sono molteplici. Si distingue, in particolare, tra gli Autori che tengono separato il contratto di fornitura del bene o del servizio dall'atto unilaterale con cui l'interessato autorizza il trattamento dei propri dati personali e coloro che configurano l'esistenza di un vero e proprio sinallagma tra la prestazione del consenso al trattamento dei dati personali e i servizi forniti dal titolare. Per la prima posizione, v. A. ADDANTE, *La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali*, in *Giust. civ.*, 2020, 889 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., ma anche, con varietà di accenti, S. PAGLIANTINI, *L'attuazione minimalista della dir. 2019/770/UE: riflessioni sugli artt. 135 octies - 135 vicies ter c. cons. La nuova disciplina dei contratti b-to-c per la fornitura di contenuti e servizi digitali*, in *Nuove leg. civ. comm.*, 2022, 1499 ss.; G. RESTA, *Contratto e diritti fondamentali*, in *Enc. dir., I Tematici: il contratto*, Milano, 2021, 291 ss., spec. § 9; C. CAMARDI, *Contratti digitali e mercati delle piattaforme. Un promemoria per il civilista*, in *Jusciv.*, 2021, 870 ss.; S. THOBANI, *Diritti della personalità e contratto. Dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018, 158 ss. Per

Anzitutto, vanno menzionate alcune recenti pronunce dei giudici amministrativi, che nel presupporre che i dati personali avessero la natura di utilità patrimoniali, suscettibili di formare oggetto di "scambio" e, inoltre, di rapporti di consumo, hanno sottolineato la necessità di preservare la libertà dell'interessato chiamato a decidere se fornire o meno le informazioni che lo riguardano[9].
Anche la giurisprudenza civile non ha escluso la possibilità di "scambiare" dati personali contro servizi, affermando, al contempo, la necessità che la libertà del consenso dell'interessato sia rigorosamente accertata[10]. Con la nota pronuncia del 2 luglio 2018, n. 17278 (c.d. "caso AdSpray")[11], la Corte di cassazione ha affermato, con riferimento alla condizionalità del consenso al trattamento, alcuni importanti principi.
In primo luogo, quello per cui è "da escludere che il consenso (…) sia semplicemente il medesimo consenso in generale richiesto a fini negoziali", tanto che il medesimo è "tale da non ammettere compressioni di alcun genere e non sopporta di essere sia pure marginalmente perturbato non solo per effetto di errore, violenza o dolo, ma anche per effetto dell'intero ventaglio di possibili disorientamenti, stratagemmi, opacità, sotterfugi, slealtà, doppiezze o malizie comunque adottate dal titolare del trattamento". Secondo la Corte, il consenso in questione va "ricondotto alla nozione di 'consenso informato', nozione ampiamente impiegata

---

la seconda posizione, v. G. BUSET, *Brevi note sull'attribuzione del godimento nel prisma della evoluzione tecnologica*, in *Jusciv.*, 2022, 511 ss.; P. GALLO, *Il consenso al trattamento dei dati personali come prestazione*, in *Riv. dir. civ.*, 2022, 1054 ss.; V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ.*, 2020, 642 ss.; R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contr. impr.*, 2020, 760 ss.; C. PERLINGIERI, *Data as the Object of a Contract and Contract Epistemology*, in *ItaLJ*, 2019, 615 ss.

[9] Al riguardo si vedano C. St., 29.3.2021, n. 2631 (che ha confermato T.A.R. Lazio n. 261/2020) e T.A.R. Lazio, sez. I - Roma, 10.1.2020, nn. 260 e 261. Quanto alla pronuncia del Consiglio di Stato, v. *Nuova giur. civ. comm.*, 2021, 1079 ss., con nota di D. D'ALBERTI, *Tutele "multilivello" e l'effettività dei rimedi per gli utenti online*, in *Resp. civ. prev.*, 2021, 1604 ss., con nota di L. CASALINI, *Dati personali all'intersezione tra diritto del consumo e tutela della privacy*; *Giustiziacivile.com*, con nota di V. RICCIUTO e C. SOLINAS, *Fornitura di servizi digitali e prestazione di dati personali: punti fermi ed ambiguità sulla corrispettività del contratto*, in *Foro it.*, 2021, 325 ss., con nota di A. D'AVOLA e R. PARDOLESI, *Protezione dei dati personali, tutela della concorrenza e del consumatore (alle prese con i "dark pattern"): parallele convergenti?*. Per quanto concerne, invece, la pronuncia del T.A.R. Lazio n. 260/2020, v. *Giur. it.*, 2021, 320 ss., con nota di C. SOLINAS, *Circolazione dei dati personali, onerosità e pratiche commerciali scorrette*; *Juscivile*, 2020, 1355, con nota di B. PARENZO, *Dati personali come "moneta"*. Infine, con riferimento a T.A.R. Lazio n. 261/2020, si rimanda a *Dir. ind.*, 2021, 511 ss., con nota di G.P. PASTUGLIA, *Prime note in materia di coordinamento tra disciplina delle pratiche commerciali scorrette e regole privacy*.
Ancor più recentemente il T.A.R. Lazio ha confermato la sanzione irrogata dall'AGCM nei confronti di Google, ritenuto responsabile di aver adottato pratiche commerciali scorrette, consistenti nel: non aver fornito agli utenti informazioni sufficientemente chiare in merito alla raccolta ed utilizzo dei loro dati personali a fini commerciali; aver preimpostato il consenso dei consumatori al trasferimento dei loro dati a Google a scopi commerciali, limitandone così fortemente la libertà di scelta in ordine alla prestazione del consenso. Si veda, in particolare, T.A.R. Lazio, sez. I - Roma, del 18.11.2022, n. 15326, disponibile su *Dejure*.

[10] Per completezza d'analisi, si segnala la decisione del Trib. Bologna, sez. II, 10.3.2021, in *Dejure*, che ha affermato l'esistenza di un sinallagma tra la fornitura di servizi di *social network* e i dati personali concessi dall'utente: "A prescindere dall'utilizzo che la resistente [Facebook] ne faccia (se li ceda e li trasmetta a terzi oppure se ne serva soltanto per offrire ai terzi i presupposti di una informazione pubblicitaria mirata), non può revocarsi in dubbio che i dati personali dell'utente abbiano un manifesto valore economico e siano inquadrabili come controprestazione nel rapporto utente-gestore (…). Ne consegue il carattere evidentemente oneroso del rapporto negoziale, posto che il contratto è fondato su un evidente sinallagma, per cui alla prestazione del servizio da parte del gestore corrisponde il suo interesse ad utilizzare i contenuti, le reti di relazioni e i dati personali dell'utente, a fini di raccolta pubblicitaria". Nella specie il ricorrente agiva in giudizio lamentando l'immotivata rimozione da parte di Facebook delle pagine di cui era titolare, rimozione che il giudice ha qualificato come "*inadempimento*", e chiedendo il risarcimento del conseguente danno.

[11] V. *Giur. it.*, 2019, 530 ss., con nota di S. THOBANI, *Operazioni di* tying *e libertà del consenso*; in *Nuova giur. civ. comm.*, 2018, 1775 ss., con nota di F. ZANOVELLO, *Consenso libero e specifico alle e-mail promozionali*.

in taluni settori – basti menzionare il campo delle prestazioni sanitarie – in cui è particolarmente avvertita l'esigenza di tutelare la pienezza del consenso, in vista dell'esplicazione del diritto di autodeterminazione dell'interessato, attraverso la previsione di obblighi di informazione". Ancora, la Corte ha rilevato che un condizionamento *ex* art. 7, 4° co., GDPR "*non* può sempre e comunque essere dato per scontato", dovendo però "essere tanto più ritenuto sussistente, quanto più la prestazione offerta dal gestore del sito Internet sia ad un tempo infungibile ed irrinunciabile per l'interessato". In definitiva, "l'ordinamento non vieta lo scambio di dati personali, ma esige tuttavia che tale scambio sia frutto di un consenso pieno ed in nessun modo coartato".
Dalla giurisprudenza passata in rassegna emerge che lo 'scambio' di dati personali non è vietato, purché l'interessato sia adeguatamente informato e non sia in alcun modo condizionato, né dal modo in cui le informazioni gli vengono fornite, né dai mezzi tecnologici a questo scopo adoperati.
Il problema risulta particolarmente delicato e complesso quando si è in presenza di una situazione di sproporzione strutturale, informativa o economica, tra l'interessato ed il titolare.
In particolare, l'attenzione si è soffermata sulle grandi piattaforme nel mercato digitale.
Su questo delicato punto si è pronunciata la Corte di Giustizia dell'UE, nell'ambito della causa C-252/21, tra il gruppo Meta Platforms e il Bundeskartellamt, l'Autorità federale garante della concorrenza tedesca. Significativamente, l'Avv. Generale Rantos, il 20 settembre 2022, concludeva nel senso che: "L'articolo 6, paragrafo 1, lettera a), e l'articolo 9, paragrafo 2, lettera a), del RGPD devono essere interpretati nel senso che la sola circostanza che l'impresa che gestisce una rete sociale goda di una posizione dominante sul mercato nazionale delle reti sociali in linea per utenti privati non può, di per sé, privare il consenso dell'utente di tale rete al trattamento dei suoi dati personali della sua validità ai sensi dell'articolo 4, paragrafo 11, del RGPD. Siffatta circostanza svolge tuttavia un ruolo nella valutazione della libertà del consenso ai sensi di tale disposizione – la cui dimostrazione incombe al titolare del trattamento – tenendo conto, se del caso, dell'esistenza di un evidente squilibrio di potere tra l'interessato e il titolare del trattamento, dell'eventuale obbligo di acconsentire al trattamento di dati personali diversi da quelli strettamente necessari per l'erogazione dei servizi di cui trattasi, della necessità che il consenso sia specifico per ciascuna finalità del trattamento e della necessità di evitare che la revoca del consenso da parte dell'utente causi a quest'ultimo un pregiudizio"[12].
Le conclusioni dell'Avvocato Generale confermano che la libertà non è sempre e in ogni caso compromessa dall'esistenza di un evidente squilibrio di potere tra le parti – l'interessato e il titolare – né dalla circostanza che il consenso viene dato in cambio della fruizione del servizio.
Questa impostazione ha poi trovato conferma nella sentenza della CGUE[13].
Ancorché indirettamente, rileva altresì quanto già affermato dalla Corte di Giustizia nella decisione dell'11 novembre 2020, resa nella causa C-61/69, il caso c.d. "Orange Romania"[14].

[12] Le osservazioni dell'Avvocato Generale si riferivano alla sesta questione pregiudiziale, ossia quella che chiedeva di chiarire "se, in generale, gli utenti possano prestare un valido consenso nei confronti di una società dominante come Facebook Ireland, ai sensi degli articoli 6, paragrafo 1, lettera a), e 9, paragrafo 2, lettera a), del RGPD, come disposto dal Bundeskartellamt per rimediare all'asserita violazione, o se la manifestazione di libera volontà richiesta a tal fine dall'articolo 4, paragrafo 11, del RGPD debba essere sempre esclusa nei confronti di una società in posizione dominante come Facebook Ireland, anche quando l'esecuzione del contratto non dipende dal consenso al trattamento dei dati".
[13] CGUE, Grande Sezione, 4.7.2023, causa C-252/21, in particolare par. 140 ss., consultabile su *https://curia.europa.eu*.
[14] La causa vedeva contrapposte l'Orange România SA, fornitore di servizi di telecomunicazione mobile nel mercato rumeno, e l'Autorità nazionale di sorveglianza del trattamento dei dati personali della Romania.

Chiamata ad indicare quali condizioni devono essere soddisfatte affinché una manifestazione di volontà possa dirsi specifica, informata e liberamente espressa[15], la Corte ha ricordato che ogni condotta decettiva o anche solo opaca, tenuta dal titolare che chieda il consenso all'interessato, ne esclude il carattere libero. La decisione non può invece essere letta nel senso di escludere, in termini assoluti, la libertà dell'interessato posto di fronte al contratto condizionato al rilascio del consenso al trattamento dei dati personali.
Dunque, sia nel caso Orange che nel caso Meta, non si esclude che il consenso al trattamento dei dati personali possa ritenersi libero, benché prestato a fronte di un servizio. In entrambi i casi, però, il giudizio è fortemente legato all'esame del contesto specifico in cui lo scambio si svolge. Si tratta, quindi, di una lettura strettamente collegata al caso per caso, alla contestualità, all'esame di tutti gli elementi in cui il consenso si forma e in cui la libertà si esplica.

4. La libertà del consenso in una dimensione contestuale.

Da quanto si è esposto, emerge che al cuore del problema sta l'individuazione delle caratteristiche della libertà.
Infatti, nel discutere dei requisiti del consenso, sia nell'ambito negoziale sia nell'ambito della protezione dei dati personali, il requisito della libertà ha già normativamente una posizione centrale, che diviene ancora più importante alla luce degli orientamenti giurisprudenziali e dottrinali sopra esposti.
Tuttavia, a ben vedere, in entrambi gli ambiti, quello negoziale e quello del trattamento dei dati personali, non si tratta di una libertà assoluta, ma limitata.
La libertà nel contratto, da tempo non coincide, o non coincide più, con la sola espressione della volontà dei contraenti[16]. Infatti, non siamo più nell'epoca della signoria della volontà, ma siamo piuttosto nell'epoca degli scambi senza accordo, come scriveva Irti[17].
Il processo di formazione della volontà e di conseguenza la valutazione del grado di libertà dei contraenti non si esaurisce nella sfera soggettiva della parte ma, invece, deve tenere in necessaria considerazione alcuni parametri esterni alla sfera del contraente.
La volontà non deve essere stata, per esempio, condizionata dalle molte fattispecie di abuso che arricchiscono la disciplina contrattuale. I vizi non sono solo i vizi del consenso previsti dal codice, che conducono all'annullabilità del contratto, ma anche quelli che, pur situati, come è stato detto, sotto la soglia dei vizi del consenso, alterano l'equilibrio contrattuale e conducono ai rimedi risarcitori[18]. Quindi l'espressione della volontà libera del contraente, in realtà, si definisce con il riferimento necessario a elementi al di fuori della sfera individuale. La locuzione "nei limiti imposti dalla legge" del codice civile oggi si colora in maniera completamente diversa, e si sostanzia differentemente l'espressione della volontà nel contratto, nella considerazione di alcune fattispecie che il legislatore euro-unitario, ma anche nazionale,

[15] Giova rilevare che la CGUE decideva la questione pregiudiziale con riferimento alla normativa abrogata dal GDPR, l'art. 2, lett. h) della Direttiva 95/46/CE. Sebbene le riflessioni della Corte riguardino la normativa non più vigente, però, sono riferibili anche al Regolamento (UE) 2016/679, in cui pure il consenso si definisce come una manifestazione di volontà libera, specifica e informata. Sulla decisione, v. C. ANGIOLINI, *A proposito del caso Orange Romania deciso dalla corte di giustizia dell'UE: il rapporto fra contratto e consenso al trattamento dei dati personali*, in *Nuove leg. civ. comm.*, 2021, 247 ss.
[16] Emblematica, sotto questo profilo, risulta la decisione di Cass., sez. I, 25.5.2021, n. 14381, soffermatasi sui requisiti di libertà del consenso al trattamento automatizzato dei dati personali strumentale all'elaborazione di profili reputazionali. La decisione è consultabile in *Dir. inform.*, 2021, 6, 1001 ss., con commento di F. BRAVO, *Rating reputazionale e trasparenza dell'algoritmo. Il caso «Mevaluate»*.
[17] N. IRTI, *Scambi senza accordo*, in *Riv. trim. dir. proc. civ.*, 1998, 347 ss.
[18] La ricostruzione delle linee essenziali di quest'evoluzione del sistema è offerta da A. GENTILI e V. CINTIO, *I nuovi "vizi del consenso"*, in *Contr. impr.*, 2018, 148 ss.

ha individuato come fattispecie di abuso. La libertà, dunque, va cercata in una dimensione ultra-individuale.
Qualche anno fa, Sacco osservava, nei suoi scritti relativi al contratto: "perché il contraente possa deliberare nel modo desiderabile bisogna che egli sia libero, abbia attitudine, capacità, tempo per ponderare, conosca e sappia, cioè sia informato"[19].
Tutto questo però, se lo "scambio" è uno scambio senza accordo, che si svolge nel breve istante di un *click*, nell'urgenza del tempo telematico, non si può realizzare. Allora la libertà non va cercata soltanto in quel *click*, ma nei presupposti, nel contesto di quello scambio e di quella relazione. La libertà va individuata in una dimensione contestuale e in questo senso propendono i recenti regolamenti europei in materia di digitale e, in particolare, il Regolamento c.d. *Digital Services Act*[20], che prevede che le piattaforme abbiano dei doveri informativi, proceduralizzino il processo di decisione e introduce obblighi per le piattaforme di intervenire, di oscurare e di sanzionare. Si sta definendo sempre di più un diverso significato di volontà e di libertà, ancora prima che nella protezione dei dati personali, proprio nel contratto.
Allora i due binari, quello del contratto e quello dei diritti della persona, non sono affatto più paralleli, ma si intrecciano e fruiscono l'uno dall'altro di letture inedite e, fino a qualche tempo fa, inimmaginabili.

[19] R. SACCO in R. SACCO e G. DE NOVA, *Il contratto,* Milano, 2016, 607 ss.
[20] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE, "Regolamento sui servizi digitali". Per un approfondimento si consenta di richiamare il mio *Responsabilità delle piattaforme e tutela dei consumatori*, in *Giornale dir. amm.,* 2023, 730 ss.

CONSENSO AL TRATTAMENTO E CONTRATTO

Di Vincenzo Ricciuto

SOMMARIO: 1. Il dibattito sul consenso al trattamento dei dati personali nelle operazioni contrattuali. – 2. Le tesi del doppio consenso e le loro criticità. - 3. Autodeterminazione informativa e autonomia contrattuale. – 4. La libertà del consenso. – 5. Conclusioni.

1. Il dibattito sul consenso al trattamento dei dati personali nelle operazioni contrattuali.

Chi oggi voglia riflettere sulla relazione concettuale e dogmatica tra consenso al trattamento dei dati personali e contratto si troverebbe a dover prendere posizione su uno dei temi più spinosi e delicati della teoria dei rapporti giuridici nella società digitale. Un tema oggi al centro del dibattito e che, da qualche tempo, impegna la riflessione degli interpreti. Questi ultimi – ora con più, ora con meno convinzione – tentano di spiegare, costruire, offrire una prospettiva giuridica del fenomeno della circolazione dei dati personali che colga appieno anche la sua reale dimensione economica, attraverso un'ottica di tipo negoziale (seppur declinata secondo profili, sensibilità, formazione scientifica e culturale diverse e variegate, che certo esprimono un attaccamento, ora più ora meno intenso, alle categorie classiche della nostra tradizione).
Così, è diventato paradigmatico il caso, appunto, del consenso al trattamento, il quale, calato nel contesto della circolazione di un valore e di un bene economico – come ormai è anche considerato il dato personale – pone la questione se esso assuma la valenza di un consenso negoziale fino a configurare l'idea di un elemento costitutivo di una fattispecie contrattuale.
Secondo una prima lettura, che, in verità, parrebbe ancorata al tradizionale approccio che esprime riserve circa la natura negoziale del consenso al trattamento dei dati, occorre tenere separati i due piani del rapporto tra le parti di un contratto nel quale sia presente un fenomeno circolatorio del dato personale: il "piano che si instaura con l'accordo negoziale" e il piano del "rapporto tra interessato e titolare del trattamento, che si instaura con il consenso del primo e si muove lungo le linee di una disciplina di fonte prevalentemente legale e di carattere essenzialmente imperativo"[1].
La tesi separa, nell'ambito dell'operazione economica, il momento del consenso contrattuale - in cui si conclude il contratto relativo al bene o al servizio - dal momento del consenso all'uso dei dati personali, ipotizzando così una differenza di rapporto e natura.
L'approdo di tal ragionamento è che il consenso al trattamento non è elemento del contratto, ma è ad esso estraneo[2].

---

[1] E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e impresa*, 2018, 113 ss.

[2] C. IRTI, *Consenso «negoziato» e circolazione dei dati personali*, Torino, 2021, 77, la quale individua una "duplicità dei piani disciplinari, che comportano l'esigenza di tenere ben distinte, all'interno di quella che si presenta come un'unica manifestazione di volontà, il consenso autorizzativo a carattere unilaterale, che viene «scambiato» al fine di ottenere il prodotto o il servizio, e il consenso negoziale quale dichiarazione adesiva dell'utente al regolamento che disciplina il rapporto". Mitiga la nettezza della separazione delle due fattispecie di consenso, R. SENIGAGLIA, *Minore età e contratto. Contributo alla teoria della capacità*, Torino, 2020, il quale parla di consenso contrattuale e consenso al trattamento come di elementi di un un'unica fattispecie che "dà luogo ad un atto *oggettivamente complesso*". Sulla diversità strutturale dei due atti, cfr. anche I.A. CAGGIANO, *Il*

Tuttavia, sviluppate nelle loro coerenti conseguenze, le ricostruzioni attraverso le quali si 'salva' il profilo personalistico[3] (sottraendolo alla ricostruzione in chiave di consenso contrattuale) rischierebbero di rendere gli attributi della persona le sole 'utilità' che, in quella data operazione, circolano, senza che il soggetto al quale i dati si riferiscono possa beneficiare, in cambio, di alcuna controprestazione da parte dell'impresa fornitrice.
Non solo: in realtà il mantenimento di un consenso fuori o/e autonomo e di natura diversa da quello contrattuale non scioglie gli equivoci che caratterizzano questa tematica: la prospettiva rischia di essere quella di una lettura che, se da un lato rende possibile, con il consenso della persona, il fenomeno economico del trattamento, dall'altro ne prende le distanze non volendo rassegnarsi a vedere la persona stessa coinvolta in una vicenda negoziale. In altri termini, ancora, ci troveremmo dinnanzi al tentativo, pur lodevole, di un recupero della dimensione dei diritti della persona senza la sua compromissione in un fenomeno economico e di mercato.
Ed ancora, in sostanza, secondo una tale ricostruzione, la dimensione del consenso in materia di trattamento dei dati personali dettata o ricavabile dal GDPR sarebbe del tutto specifica e peculiare (peculiarità di cui darebbe conto non solo l'art. 8, in tema di consenso del minore di età[4], ma altresì l'art. 7 GDPR, laddove pone la revocabilità del consenso) e non coinciderebbe con quella del consenso contrattuale di cui al codice civile.

---

consenso al trattamento dei dati personali nel nuovo Regolamento europeo, in *Oss. Dir. Civ. Comm*., 2019, spec. p. 86. E. LUCCHINI GUASTALLA, *op. cit.*, cit., 116 ss.

[3] Sulla compresenza dei piani "personalistico" e "patrimoniale" nella vicenda circolatoria dei dati personali, allorquando si realizzino fenomeni economici di circolazione della ricchezza, ho avuto modo di sviluppare più ampie riflessioni, alle quali rinvio, in V. RICCIUTO*, L'equivoco della privacy. Persona vs dato personale*, Napoli, 2022.

[4] Proprio dalla norma in tema di consenso al trattamento dei dati del minore di cui all'art. 8 GDPR, le tesi che ragionano di un doppio consenso, traggono conferma delle proprie ricostruzioni. Per i servizi della società dell'informazione e, pertanto nel contesto dell'economia digitale, infatti, il consenso al trattamento dei dati personali è validamente prestato a 16 anni (art. 8 GDPR). Se il sedicenne può acconsentire al trattamento dei propri dati (e se questi sono il valore di scambio dei servizi offerti nella società digitale) si dovrebbe concludere, in via logica, che il GDPR ha abbassato la capacità di agire per questa particolare ipotesi di contratti. Il limite di età al consenso al trattamento va coordinato, però, con il § 3 dell'art. 8, a norma del quale sono invece fatte salve le norme generali in materia di diritto dei contratti.
Ebbene, l'ipotesi di una separazione tra i due consensi (al trattamento e al contratto) condurrebbe a questo risultato: vi è un contratto per il quale rimane ferma la disposizione di carattere generale (la capacità di agire posta alla maggiore età) e accanto ad esso vi è un secondo atto, il consenso al trattamento, per il quale è introdotta una età inferiore. Per le tesi sopra riferite proprio una tale netta separazione riuscirebbe a spiegare e a sciogliere il problema di coordinamento posto tra i differenti limiti di età del consenso individuati da un lato dal GDPR e, dall'altro lato, dal Codice civile. Piuttosto che leggere nell'art. 8 una norma che ha posto una capacità speciale per i contratti della società digitale nei quali il minore dispone dei propri dati (pur facendo salva la disciplina generale in tema di contratti), le tesi *de quibus* hanno pertanto ipotizzato uno sdoppiamento dei consensi che, in definitiva, realizzano l'operazione economica.
Ma non può che riscontrarsi l'insostenibilità reale di tale ipotesi dogmatica. L'idea di un contratto stipulato da un sedicenne che, parallelamente ad esso, per accedere al servizio digitale (al giochino sul cellulare) fornisce il consenso al trattamento dei propri dati personali, si tradurrebbe, a ben vedere, nell'ipotesi di un contratto (per la fornitura del giochino) invalido (perché stipulato dal sedicenne), e di un atto di consenso al trattamento dei dati personali, al contrario, valido e tutelato dall'ordinamento giuridico. L'effetto paradossale è che il fornitore del servizio potrebbe lecitamente trattare i dati del sedicenne, senza essere obbligato a fornire in cambio il servizio digitale. Il che sembrerebbe andare in senso contrario a ciò che la sola prospettiva personalistica vorrebbe ottenere in termini di tutela nel tentativo del difficile bilanciamento tra le istanze personalistiche e patrimoniali del soggetto. L'assunto di partenza (naturalmente del tutto condivisibile) è che la persona è irriducibile ad una merce; conclusione questa che non si estende ai (suoi) dati personali che, invece, come è ormai acquisito possono essere un corrispettivo per le forniture contrattuali .

In altri termini – e per dirla ancora più nettamente – secondo queste impostazioni vi sarebbe un consenso con cui si conclude il contratto, che sarebbe concettualmente ed operativamente distinto da un diverso consenso al trattamento dei dati personali[5].
Quello contrattuale è un consenso con il quale un utente ottiene la fornitura di un servizio: un contratto che avrà ad oggetto, secondo queste letture, l'obbligo dell'impresa ad erogare il servizio e, al contempo, l'impegno (si badi: non l'obbligo) dell'utente ad esprimere il proprio consenso al trattamento dei dati personali.
Il consenso al trattamento sarebbe, dunque, un diverso consenso con il quale l'utente attribuisce al fornitore del servizio la possibilità di trattare i suoi dati personali. E, d'altra parte, proprio ragionare di una relazione tra consenso al trattamento dei dati personali e (consenso al) contratto farebbe pensare ad un'impostazione di questo tipo, concependo i due momenti come distinti non solo sul piano descrittivo, ma altresì su quello operativo e dogmatico.
Considerati insieme, dal punto di vista sostanziale, i due consensi realizzano lo scambio servizi/dati; tuttavia, il consenso al trattamento dei dati personali non sarebbe elemento costitutivo del contratto di scambio stesso. Così si parla di un consenso autorizzativo a carattere unilaterale, che viene scambiato al fine di ottenere il prodotto-servizio, e di un consenso negoziale quale dichiarazione adesiva dell'utente al regolamento che disciplina il rapporto.
L'operazione economica di scambio è, insomma, sì riconosciuta[6], ma si intende realizzata attraverso due diversi atti e due diverse manifestazioni di consenso dell'interessato/utente[7].

---

[5] Secondo G. RESTA, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la dottrina (UE)2019/770 e il Regolamento (UE) 2016/679,* in *Forniture di servizi digitali e «pagamento» con la prestazione dei dati personali. Un discusso profilo dell'economia digitale*, a cura di V. Ricciuto e C. Solinas, Milano, 2022, 74 ss. il consenso al trattamento costituirebbe un atto a struttura unilaterale, che funzionalmente realizzerebbe l'esercizio del diritto di "autodeterminazione informativa", così "la disciplina forgiata dal legislatore comunitario indica chiaramente che il consenso non può essere parificato ad un qualsiasi altro atto negoziale". Il consenso al trattamento sarebbe "giuridicamente più prossimo al consenso informato al trattamento medico che non al prototipo degli atti negoziali a contenuto patrimoniale", sicché per questo Autore il consenso al trattamento dei dati opera quale scriminante della liceità del trattamento e non assurgerebbe a elemento di una fattispecie negoziale, così che il contratto di scambio tra servizio e dati opererebbe solo "a valle" rispetto al primo consenso, e solo a quel punto assurgerebbe a figura contrattuale.
Pur nella individuazione di un "doppio consenso" – uno riferito al trattamento, l'altro al contratto di fornitura dei servizi – secondo C. IRTI, *op. cit.*, 90, nel caso dello scambio dati/servizi, "l'«oggetto» del contratto è rappresentato dal complesso delle prestazioni dedotte – fornitura di un servizio o di un contenuto digitale vs. rilascio del consenso all'utilizzazione dei dati forniti». Per l'Autrice, il consenso al trattamento dei dati costituisce dunque una prestazione avente fonte nel contratto di servizi. Il GDPR avrebbe così il pregio di valorizzare "un modello contrattuale composto da due momenti negoziali diversi e distinti, seppur collegati nel contesto di un'operazione economica unitaria" implicando "un doppio procedimento formale e di un doppio consenso da parte dell'utente del servizio innanzitutto il procedimento e il relativo consenso concernenti la conclusione del contratto di fornitura (sottoposto alle ordinarie regole contrattuali); e poi il procedimento concernente la raccolta del consenso informato e l'esplicazione analitica delle finalità del trattamento, sottoposto alle puntuali e rigorose regole del GDPR": così C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione dei dati personali*, in *Giust. civ*., 2019, 510 ss.
[6] V., ancora, C. IRTI, *Recensione a V. Ricciuto, L'equivoco della privacy*, in *AdC*, 2022, 325, la quale – pur nella diversità degli esiti interpretativi – condivide molti dei rilievi che ho posto in luce, sin già nel mio volume *L'equivoco della privacy*, cit.: "il fatto che la protezione dei dati personali non si identifichi con quella della riservatezza nonché con la privacy così come intesa nella sua accezione originaria; il riconoscimento dei dati personali come beni suscettibili di essere sfruttati per finalità patrimoniali, senza che questo sfruttamento implichi la necessaria cessione del «bene» (di per sé incedibile); la necessità che all'operazione economica sottesa allo sfruttamento di questi beni «speciali» sia applicata in funzione conformativa quella disciplina di settore di matrice sovranazionale destinata alla loro protezione".
[7] V., ancora, C. IRTI, *Recensione*, cit., 324, ove è sì operata una ricostruzione delle "operazioni economiche digitali che si perfezionano nello scambio tra la prestazione del consenso al trattamento dei dati e il servizio o prodotto digitale (apparentemente offerto come 'gratuito') nell'ambito del contratto", ma si riafferma come "necessario tenere distinti - in quanto concettualmente ed operativamente diversi – il consenso con il quale si conclude il contratto per la fornitura del prodotto o servizio digitale dal consenso al trattamento dei dati personali, lì dove

Solo un consenso si esprimerebbe in prospettiva bilaterale con la conclusione del contratto che costituisce il rapporto patrimoniale tra fornitore del servizio ed utente e ha come propri effetti quelli di far sorgere il diritto dell'utente alla prestazione digitale. In questo contesto, il consenso contrattuale espresso dall'utente non sarebbe rivolto a concedere al fornitore dei servizi il trattamento dei dati personali ma 'solo' a concludere il contratto con il quale l'utente otterrà la prestazione digitale e si vincolerà a fornire, separatamente, il proprio consenso al trattamento dei dati personali in cambio.

2. Le tesi del doppio consenso e le loro criticità.

Ipotizzato che alla sostanza economica dello scambio corrisponda, sul piano giuridico, una duplicità di strutture (il contratto da un lato e il consenso al trattamento, dall'altro), lo schema contrattuale da taluno proposto è dunque quello del contratto con obbligazioni del solo proponente, dal momento che, per questa tesi, con il contratto l'utente non si 'obbliga', in senso proprio, a concedere il consenso al trattamento dei propri dati (art. 1333 c.c.)[8].
Tale 'impegno' dell'utente a rilasciare il consenso al trattamento dei dati, assunto con contratto, secondo le citate ricostruzioni, non potrebbe costituire una prestazione in senso tecnico – e dunque obbligatoria – poiché la volontà di fornire i dati sarebbe un'attività che giuridicamente deve restare libera ed incoercibile nel suo determinarsi. Salvo poi ammettere che una tale prestazione finisce per assumere una valenza programmatoria negoziale nel momento in cui essa assume il valore di presupposto necessario per conseguire l'attribuzione promessa in cambio (vale a dire la fornitura)[9]. Ed in ciò sta la prima criticità di queste ricostruzioni, dal momento che, in ogni caso, la fornitura dei dati personali è comunque contrattualmente, consensualmente, volontariamente programmata in funzione dello scambio (seppur eventuale, per questa ipotesi) con un dato servizio[10].
Ulteriormente sintetizzando, per le teorie che ragionano di un doppio consenso, le parti stipulano un contratto con il quale assumono, rispettivamente, il fornitore l'obbligo di erogare il servizio e l'utente l'impegno ad esprimere in cambio, successivamente (almeno dal punto di vista logico concettuale, se non temporale), il proprio consenso al trattamento dei dati personali.
L''impegno' a fornire il consenso al trattamento dei dati personali, tuttavia, non avrebbe, secondo tali ricostruzioni, struttura obbligatoria perché il consenso al trattamento dei dati personali è sempre attività libera, dunque non coercibile né preventivamente vincolabile. Da qui, il suggerimento di parlare a riguardo non di una prestazione obbligatoria al consenso al trattamento, ma di una 'prestazione condizionale', ovvero di una prestazione non assicurata dalla possibilità dell'esecuzione coattiva, ma che l'utente avrebbe comunque necessità di effettuare al fine dell'ottenimento del prodotto e/o servizio[11].

---

quest'ultimo, per quanto condizionalmente prestato al fine di ottenere l'erogazione del servizio 'gratuitamente' offerto dal fornitore, non è e non potrebbe essere oggetto di una vera e propria obbligazione suscettibile di esecuzione coattiva".
[8] C. IRTI, *Consenso,* cit., 109.
[9] C. IRTI, *op. loc. ult. cit.*
[10] In termini simili, anche S. ORLANDO, *Il coordinamento tra la Direttiva 2019/770 e il GDPR. L'interessato-consumatore,* in *Pers. merc.*, 2023, 231, il quale nota che "postulare un doppio consenso è contrario alla realtà della manifestazione dei comportamenti, ed è inoltre incompatibile con la teoria del contratto, perché, attenendo la fornitura dei dati personali all'oggetto e (…) anche alla causa del contratto, non si può immaginare un consenso contrattuale che non investa questi elementi".
[11] Così C. IRTI, *Consenso*, 103, secondo la quale "quel che manca per qualificare il rapporto in termini strettamente obbligatori è la bilateralità del vincolo giuridico, non essendo e non potendo mai essere, la prestazione gravante sul consumatore - il rilascio del consenso al trattamento del dato per finalità estranee al servizio o prodotto ricevuto

L'intento di conciliare gli aspetti personalistici nella vicenda della circolazione dei dati personali con quelli di stampo patrimoniale è sicuramente apprezzabile e, per taluni versi, condivisibile ove soprattutto si voglia, ad un primo impatto, farsi carico della preoccupazione che la natura così speciale del bene debba poter circolare patrimonialmente con particolari cautele ed attenzioni, non assimilabili a tutte le altre ipotesi di circolazione negoziale di utilità e risorse economiche: da un lato, gli aspetti di tutela della persona (presidiati, in questa impostazione, dal mantenimento dell'idea di un consenso unilaterale al trattamento dei dati personali che viaggia parallelo rispetto alla fonte del rapporto patrimoniale ed è sostenuto da c.d. principio di autodeterminazione informativa); dall'altro, gli aspetti di carattere patrimoniale (rappresentati dalla conclusione di un contratto con cui l'utente ottiene la fornitura impegnandosi, ma senza obbligarsi, a rilasciare in cambio il consenso al trattamento, sostenuto ovviamente dal principio di autonomia privata).
Però, una tale impostazione rischia di non offrire una chiave di lettura e soprattutto una prospettiva sistematica per cogliere la portata dei nuovi fenomeni patrimoniali[12].
Accanto alle suddette preoccupazioni, si scorge la tendenza a ricostruire una vicenda circolatoria di carattere patrimoniale, quale quella relativa all'ipotesi di scambio dei dati personali, che muove dall'idea che ogni decisione di un soggetto in ordine ai propri dati personali debba esaurirsi nel (limitato) orizzonte della c.d. autodeterminazione informativa, alla quale, sulla scia dell'esperienza tedesca, si è fatto riferimento in sede di interpretazione della l. n. 675/1996[13]. Il contesto nel quale tali originarie posizioni trovavano un qualche fondamento è però del tutto modificato da un punto di vista, intanto, normativo (con le modifiche alla originaria disciplina della l. n. 675/1996, la quale del tutto marginalmente si preoccupava delle vicende circolatorie); dalle letture che gli interpreti hanno successivamente offerto del fenomeno e, ancora di più, dall'erompere del fenomeno del trattamento dei dati nelle attività economiche e che ha portato all'adozione del Regolamento il quale, invece, offre (certo non esclusivamente) gli strumenti per una ricostruzione in chiave pienamente patrimonialistica e negoziale.
Ma d'altra parte, lo stesso Stefano Rodotà, a ridosso del recepimento della Direttiva del 1995, nel sottolineare l'importanza della dimensione negoziale del fenomeno affermava che, quanto al consenso negoziale, "il problema capitale è quello dell'asservimento definitivo", rilevando, proprio nelle prime applicazioni della disciplina della l. n. 675/1996, che "naturalmente la legge offre molti spunti per dire che questo asservimento definitivo non è accettato". Nella dimensione negoziale "il controllo non viene perduto, i motivi legittimi per i quali si può impedire la comunicazione di dati pur legittimamente raccolti, pertinenti o assentiti in tutto o

dall'operatore economico (titolare del trattamento oggetto) - oggetto di una obbligazione giuridicamente coercibile".

[12] Condivide queste perplessità anche S. ORLANDO, *op. cit.*, 222 ss. L'Autore citato rileva, innanzitutto, che ragionare di un c.d. doppio consenso (e dunque ritenere che la prestazione del consenso al trattamento sarebbe essa stessa 'oggetto' del contratto di scambio) sarebbe frutto di una "*interpretazione anti-letterale*" delle disposizioni che disciplinano queste operazioni (art. 3, dir. 770/2019 e, ora, art. 135 *octies*, co. 4, cod. cons.). Convince soprattutto il rilievo dell'Autore citato in ordine al fatto che la tesi del c.d. doppio consenso "sostanzialmente fa leva sull'osservazione dell'inutilità di fornire dati personali senza il consenso al relativo trattamento", laddove, invece, "proprio sulla base della pacifica osservazione per la quale il consenso è necessario al trattamento, può e deve ritenersi, in senso conforme al significato letterale della norma, che il (necessario) consenso al trattamento precede e giustifica (ove valido, naturalmente: v. infra) tanto la fornitura dei dati personali che, eventualmente, il loro impegno a fornirli".

[13] "L'atto mediante il quale il soggetto autorizza il trattamento dei propri dati personali, il consenso informato, non equivale ad un atto di disposizione, ma è e resta un atto mediante il quale il soggetto manifesta il potere di autodeterminarsi rispetto alla divulgazione e all'utilizzo da parte di terzi di informazioni che riguardano la sua sfera più personale e che non a caso il Garante ha qualificato quale «diritto all'autodeterminazione informativa»": Garante per la protezione dei dati personali, provv. del 28 maggio, 1997, in *Foro It.*, 1997, III, 317.

in parte dimostrano quindi che c'è una scelta dell'interessato che definisce l'area della protezione"[14].
L'autodeterminazione informativa, se un senso ed una funzione può aver avuto in termini assorbenti rispetto ad ogni altro principio e giustificazione delle scelte in ordine ai dati personali, deve essere concettualmente collocata coerentemente in quel contesto normativo e culturale, fortemente, se non esclusivamente, ancorato alla ricostruzione in termini solo assolutistici della tutela della persona e in chiave di tutela extracontrattuale. Ma, come le stesse parole di Stefano Rodotà chiariscono, anche in quel contesto non vi era ragione logica per escludere la compatibilità tra la dimensione negoziale del consenso e la tutela dei diritti della persona.
Oggi, in un del tutto mutato contesto, più decisamente ispirato ai principi della circolazione e patrimonializzazione dei dati, il dato circola 'protetto' per l'immanenza di quel diritto in tutte le ipotesi di circolazione, siano esse riconducibili alle ipotesi extracontrattuali o contrattuali.

3. Autodeterminazione informativa e autonomia contrattuale.

Quanto sopra detto, porta anche ad escludere che l'autonomia informativa supplisca all'autonomia contrattuale, laddove si ritiene che la "regola della circolazione dei dati personali è frutto di una decisione libera e autoreferenziale del titolare dei dati medesimi"[15]. La formula dell'autodeterminazione informativa, in quanto inidonea ad offrire piena evidenza alla funzione economica delle scelte del soggetto e dunque incapace di offrire risposta al principio della giustificazione causale che necessariamente regola, nel nostro ordinamento, la circolazione e l'attribuzione della ricchezza, non può tecnicamente dare fondamento al fenomeno, inarrestabile, ma controllabile, dell'economia dei dati.
La prospettiva di scambio di ricchezze non può essere ricondotta a concetti fondati sulla mera autoreferenzialità delle scelte, che prescinda dalla valutazione richiesta dal principio di necessaria giustificazione causale delle attribuzioni patrimoniali posto dal nostro ordinamento[16]; quest'ultima potrà essere invocata, naturalmente, quale principio che muove le

[14] S. RODOTÀ, *Conclusioni*, in *Trattamento dei dati e tutela della persona*, a cura di V. Cuffaro, V. Ricciuto e V. Zeno Zencovich, Milano, 1998, 308.
[15] R. MESSINETTI, *Circolazione dei dati personali e autonomia privata*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di N. Zorzi Galgano, Padova, 2019, 148 e già ID., *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. Crit. Dir. Priv*., 1998.
[16] Cfr. C. SOLINAS, *Autonomia privata e regolazione pubblica nel trattamento dei dati personali*, Bari, 2022, 97 ss., la quale opportunamente segnala che "nel caso del diritto al trattamento come corrispettivo l'informazione relativa al tipo di trattamento e alla qualifica del contratto è, e deve essere, fornita in quanto essa è connessa e utile per l'esercizio consapevole di una scelta economica del consumatore"; pertanto, la comprensione dei meccanismi dell'economia digitale e delle decisioni che l'interessato assume in ordine alla vicenda circolatoria dei propri dati personali non possono sempre ridursi a profili di "autodeterminazione informativa" dell'interessato, quale decisione libera ed autoreferenziale dello stesso, perché "*è* proprio l'assenza di autoreferenzialità che caratterizza la decisione dell'interessato allorquando il diritto al trattamento dei propri dati attribuito in funzione di scambio con altre utilità". Prosegue l'Autrice citata affermando che "collocata nell'operazione economica di scambio, quella decisione relativa al trattamento dei propri dati si connota per la funzione economica alla quale essa aspira e che realizza", sicché una tale volontà si esprime oltre l'idea di autoreferenzialità. Anche secondo S. ORLANDO, *op. cit.*, 231, è necessario superare la limitata ottica dell'autoreferenzialità della scelta in ordine alla circolazione dei propri dati, per andare a coglierne giuridicamente il senso. Nell'attuale contesto, se si ammette e riconosce la c.d. monetizzazione dei dati personali, non si può continuare a ritenere irrilevanti ed insignificanti *a priori* i 'perché' di tali scelte. Secondo Orlando, condivisibilmente, quando si ragiona di consenso al trattamento è necessario non solo vagliare come esso si presenta (consenso "libero", "incondizionato", "inequivoco", "specifico", "espresso", "esplicito") ma anche i suoi 'perché'. Afferma, da ultimo, la necessità di operare un "controllo funzionale del consenso privacy" anche G. VETTORI, *Rodolfo Sacco e la civilistica del XXI secolo*, in *Riv. Trim. Dir. Proc Civ*., 2023, 539 ss.

decisioni del soggetto riguardano esclusivamente l'ambito della sola realizzazione della sua dimensione personalistica e comunque fuori da un fenomeno di negozialità.
Né si può mancare di sottolineare che oggi il contratto, come strumento giuridico che realizza la circolazione della ricchezza, non è più un "affare privato tra privati"[17], e dunque, già nella sua sistemazione generale, questo istituto può accogliere quelle logiche di protezione dei dati che, d'altra parte, come detto, sono già in sé immanenti allo speciale fenomeno circolatorio considerato. Così come i profili di tutela della persona stanno alla base di alcuni principi conformativi della libertà contrattuale moderna, che non appare più indiscriminata e arbitraria, basti pensare alla rilevanza del principio di non discriminazione nell'esercizio dell'autonomia privata[18].
Peraltro, è riscontrabile in più settori che, qualora vi sia la necessità di rafforzare la posizione contrattuale di una delle parti (al di là o oltre la tutela consumeristica) l'ordinamento prevede o propone forme di integrazione e supporto per la definizione dell'operazione economica, riconducibili al più generale fenomeno della c.d. autonomia privata assistita. D'altra parte, la stessa conformazione dei contratti ad opera di autorità pubbliche trova il suo fondamento nella necessità di garantire la realizzazione di interessi che, altrimenti, la sola volontà delle parti non riuscirebbe a soddisfare.
Vi sono, inoltre, motivazioni, potremmo dire, di 'realismo' che, nella ricostruzione teorica dei fenomeni in analisi, invitano ad evitare di insistere in una eccessiva valorizzazione della forma a discapito della sostanza. L'ipotesi di un doppio consenso rischia, infatti, di complicare, peraltro inutilmente, nella struttura ciò che da un punto di vista sostanziale è estremamente lineare ed inconfutabile (l'esistenza di uno scambio, la natura bilaterale, il rilievo economico delle scelte relative al trattamento dei dati, la qualificazione di questi ultimi in termini di corrispettivo contrattuale, come del resto una ormai copiosa giurisprudenza riconosce)[19]. Un tale approccio non solo complica (nella struttura) la comprensione dei fenomeni, ma probabilmente non facilita il dialogo tra i vari ordinamenti interessati in vicende che sono, e saranno sempre più, vicende non confinate in ambiti ricostruttivi dogmatici, com'è certamente quello italiano, ma ormai disciplinate in contesti, come quello europeo, dove le scelte normative di governo di questi fenomeni superano la rigidità delle categorie formali. Ne è in fondo un esempio proprio il GDPR, che prescinde da ogni qualificazione delle situazioni giuridiche soggettive in cui il fenomeno si articola.

---

[17] Cfr. V. RICCIUTO, *Regolazione del mercato e "funzionalizzazione" del contratto,* in *Studi in onore di Giuseppe Benedetti*, Napoli, 2007, 1618, e v. anche M. ANGELONE, *Regolazione "indipendente" del mercato e "conformazione in chiave protettiva" del contratto*, in *Riv. dir. imp*., 2016, 105. Il tema apre al diritto privato regolatorio e alla regolazione del contratto: sul tema del contratto 'amministrato', v. C. SOLINAS, *Il contratto "amministrato". La conformazione dell'operazione economica privata agli interessi generali*, Napoli, 2018. Sul diritto privato regolatorio A. ZOPPINI, *Diritto privato vs diritto amministrativo (ovvero alla ricerca dei confini tra Stato e mercato)*, in *Riv. Dir. Civ*., 2013.
[18] Su questo aspetto A. GENTILI, *Il principio di non discriminazione nei rapporti civili*, in *Riv. crit. dir. priv*., 2009, 207 s.; E. NAVARRETTA, *Principio di uguaglianza, principio di non discriminazione e contratto*, in *Riv. dir. civ*., 2014, 547 ss.; G. CARAPEZZA FIGLIA, *Divieto di discriminazione e autonomia contrattuale*, Napoli, 2013. Sul piano generale, considerazioni su tale principio, in P. RESCIGNO, *Il principio di eguaglianza nel diritto privato (a proposito di un libro tedesco)*, in *Riv. trim. dir. proc. civ*., 1959, 1515 ss.
[19] Esprime perplessità su una distinzione tra piano contrattuale e piano della circolazione dei dati personali anche S. THOBANI, *I dati personali forniti «in occasione» della fornitura*, in *Forniture di servizi digitali e «pagamento» con la prestazione dei dati personali. Un discusso profilo dell'economia digitale*, a cura di V. Ricciuto e C. Solinas, Milano, 2022, 155 ss., secondo la quale "tale prospettiva dogmatica (…) fa salva in effetti la teoria non negoziale dell'operazione economica concernente la fornitura dei dati personali ad opera del consumatore. Sebbene una simile distinzione (…) risponda all'esigenza di conformarsi alla posizione dell'EDPS, ciò non può che apparire in contrasto con l'obiettivo di disciplinare in modo coerente ed organico la materia della fornitura di contenuto e servizi digitali".

Ma, soprattutto, il rilievo, in verità, riguarda il più generale approccio al tema del diritto privato europeo, che necessita indubbiamente di una maggiore definizione delle categorie concettuali, senza tuttavia arrivare ad estremizzare e operare una superfetazione della realtà fino a ipotizzare una non piena corrispondenza tra la sostanza (bilaterale e di scambio) e la forma (duplice, contestualmente bilaterale negoziale e unilaterale autorizzativa) al solo fine, mi pare, di salvare alcuni aspetti che, in verità, non vengono, per questo, 'attentati' dalla ricostruzione del fenomeno in termini contrattuali, sia sostanziali che strutturali.

4. La libertà del consenso.

Quella della libertà del consenso al trattamento dei dati è una delle preoccupazioni che muovono coloro che ipotizzano la presenza di un autonomo e separato consenso al trattamento rispetto a quello per il contratto. E la garanzia della libertà passerebbe solo attraverso la ricostruzione del consenso come libera determinazione unilaterale del soggetto[20].
L'idea che il consenso al trattamento dei dati personali come consenso contrattuale, finalizzato a porre e a realizzare lo scambio, metta in pericolo il predicato di libertà del consenso (libertà che, come noto, deve sostenere il consenso al trattamento dei dati personali) rischia di offrire una ricostruzione fuorviante del fenomeno della circolazione negoziale dei dati. Essa suggerisce l'idea che il requisito di libertà non sia predicabile per il consenso contrattuale, il quale quindi si porrebbe fuori da processi di autodeterminazione della persona in ordine alla disponibilità dei beni ad essa riferibili (i dati personali, appunto) per essere invece realmente ed effettivamente libero solo fuori da una prospettiva economico-negoziale.
E tuttavia è necessario porre l'attenzione sul fatto che nessuno ha mai dubitato che il consenso contrattuale debba essere libero: anzi, esso è tradizionalmente ritenuto presidio della libertà dell'individuo; tutta la disciplina in materia di consenso contrattuale è disciplina volta a garantire la libertà dello stesso. Quindi, in primo luogo può creare qualche perplessità il fatto che nel contesto del fenomeno della patrimonializzazione dei dati personali, proprio al fine dichiarato di garantire la libertà del consenso al trattamento, si avverta a volte la tendenza a sottrarre la scelta di concedere il trattamento dei dati in cambio di un servizio alla sua riconduzione nella categoria del consenso negoziale (per ipotizzare, quindi, che solo fuori dal contratto esista un'area di libertà nella quale il consenso può essere unilateralmente manifestato da parte dell'interessato).
D'altra parte, in una non più recente sentenza della Corte di Cassazione del 2018 (n. 1728) – peraltro resa in applicazione della precedente normativa del codice sulla protezione dei dati personali – è riconosciuto che alla base del consenso al trattamento vi è "uno scambio" di dati personali. Scambio che, secondo la Cassazione, non è vietato dall'ordinamento, il quale certamente "esige (…) che tale scambio sia frutto di un consenso pieno ed in nessun modo coartato". In quella sentenza la Corte di Cassazione configura, rispetto al fenomeno contrattuale, un'ipotesi di consenso che, pur nella sua specialità conseguente alla particolare

[20] Scrive G. RESTA, *op. cit.*, 75 ss.: "i requisiti della «libertà», dell'«informazione» e della «specificità» fissano uno standard di validità – nel senso di idoneità a produrre l'effetto legittimante di cui all'art. 6 del regolamento – che è molto più elevato rispetto a quello consueto per gli atti patrimoniali ed è volto a garantire che l'atto veicoli una reale determinazione volitiva del soggetto», sicché per l'Autore "ne discende l'esigenza di un trattamento differenziato dei due atti giuridici coinvolti: come si è chiarito in precedenza, il consenso è soggetto alla disciplina del regolamento, ha una sua specificità ed è connotata dagli elementi precedentemente illustrati, mentre il contratto è soggetto alle diverse regole derivanti dal diritto interno e dalle fonti europee, siano queste le regole generali o quelle preordinate alla tutela dei consumatori".

natura del bene (un consenso informato, pieno, consapevole, specifico), si deve ricondurre pur sempre ad elemento di una fattispecie negoziale[21].
Nell'esperienza del diritto civile contemporaneo, peraltro, si riconosce e si ammette (senza dubbio alcuno, visto che è la stessa normativa speciale in tema di contratto che lo prevede) che sarebbe improprio ipotizzare che esista un unico modello di consenso contrattuale. Il diritto dei contratti moderno presenta una varietà di consensi, retti da discipline differenti in quanto aventi ognuno una propria specifica esigenza regolamentare, ma tutti ritenuti liberi e comunque pacificamente riconducibili alla natura contrattuale (es. consenso informato, consenso del minore, consenso del consumatore, consenso delle piccole e medie imprese non condizionabile da pratiche commerciali sleali, ecc.).
E poi, una tesi che ipotizzi che oltre al consenso contrattuale vi sia un secondo consenso con il quale l'interessato fornisce i dati, non risolve il problema della comprensione e disciplina dello scambio dati/servizi e delle tutele. Se, come ritenuto dalle impostazioni che costruiscono l'ipotesi di un 'doppio consenso', lo scambio di dati contro forniture non si realizza attraverso il solo consenso contrattuale, ma attraverso un'ulteriore manifestazione di consenso che sia precedente o successiva ad esso, quale sarebbe la natura di una tale manifestazione di volontà? È la fonte di una prestazione isolata, che si colloca fuori da una giustificazione causale di quella operazione economica di fornitura di servizi e fornitura di dati? Oppure vi è un collegamento negoziale tra contratto di fornitura e atto (ma, a questo punto, anch'esso necessariamente negoziale!) di rilascio del consenso al trattamento nell'ambito di un'operazione economica complessa?

5. Conclusioni.

Al di là delle acute e suggestive ipotesi ricostruttive di cui si è detto, la circolazione del dato personale ha fonte in – e dà luogo ad – una fattispecie contrattuale a tutti gli effetti: il consenso è uno solo, inequivocabilmente elemento di una fattispecie negoziale[22]; i profili di specialità sono riconducibili alla peculiarità dello scambio (perché speciale è il bene che ne è l'oggetto), ma senza che tale circostanza imponga anche solo logicamente di condurre fuori dall'ambito negoziale in senso stretto il fenomeno.
In sostanza, nelle ipotesi in cui si assiste ad una vicenda di corrispettività ed onerosità tra beni/servizi e dati personali si è in presenza di una fattispecie contrattuale che non necessita di ulteriori elementi costitutivi di quegli effetti giuridici. Pertanto, attribuire efficacia costitutiva del diritto a trattare i dati personali ad un elemento esterno alla fattispecie contrattuale, prima

[21] Come nota anche S. ORLANDO, *op. cit.*, 231, "contrariamente a quanto si tende a cogliere nella già citata sentenza della Cassazione 17278/2018, nessuna insormontabile differenza di natura è correttamente postulabile tra consenso privacy e consenso negoziale, e contrattuale in particolare. La teoria del contratto ammette senz'altro al suo interno forme di manifestazione della volontà contrattuale 'rafforzate' (per usare l'aggettivo che si legge al punto 2.4 di quella sentenza) per previsione di norme imperative. In particolare, e venendo al nostro caso, non è incompatibile con la teoria del contratto interpretare gli artt. 4 n. 11 e 6(1)(a) del GDPR in combinato disposto con l'art. 3(1) DCD nel senso di ritenere che nei contratti previsti da quest'ultima disposizione il consenso del consumatore-interessato debba consistere in una manifestazione di volontà libera, specifica, informata e inequivocabile, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento, con le modalità e per le finalità previste nel contratto e, sempre, beninteso, nei limiti imposti dalla legge".
[22] Adesivo, A. MORACE PINELLI, *Introduzione*, in *La circolazione dei dati personali: persona, contratto e mercato*, a cura di A. Morace Pinelli, Pisa, 2023, 13, secondo il quale il consenso è uno solo: conclude il contratto e, al contempo, ne autorizza il trattamento; i profili di specialità di un tale consenso trovano giustificazione nella peculiarità della natura del bene scambiato.

o dopo di questa, per quanto a quest'ultima connessa, non serve ad esprimere la portata, l'ambito e gli effetti che realizza quell'operazione economica.
Si deve ancora qui ribadire che gli strumenti, gli istituti, le tutele, le garanzie per il soggetto a cui i dati si riferiscono sono tutti interni al fenomeno dello scambio, poiché a beneficio dell'interessato la disciplina del trattamento dei dati riconosce forme di protezione: gli obblighi di informativa, la revoca del consenso, la garanzia di libertà del consenso, l'accesso ai propri dati, la rettifica, ecc.
Si deve sempre ricordare, che il 'diritto alla protezione dei dati personali' è riferito e riferibile anche alle negoziazioni che hanno ad oggetto quei beni e non è, dunque, espressione del solo profilo di tutela della personalità secondo la tradizionale lettura in termini extracontrattuali.
Diversamente, occorrerebbe capire come sarebbe possibile fornire rilevanza a tutte quelle circostanze che alterano la comprensione, la volizione, la corretta ponderazione della scelta in ordine al fornire i propri dati personali in una prospettiva di scambio. Se, in un contesto di scambio, appunto, la decisione di fornire i propri dati personali fosse una mera e sola scelta unilaterale, dalla quale pertanto non emerge né rileva per il diritto alcuna destinazione funzionale ad uno scambio, allorquando l'interessato cada in errore o non sia posto nelle condizioni di rendersi conto della convenienza economica di quella scelta, egli finirebbe per non avere le tutele proprie di ogni fenomeno di scambio, pure riconosciuto dalle posizioni riferite.
Significherebbe sottrarre la stessa al vaglio della sua sostenibilità e rilevanza causale (a cui sono invece sottoposte le scelte negoziali) in ordine all'assetto di interessi voluto.
L'interessato che sceglie di fornire i dati personali per accedere ad un servizio, in realtà e a ben vedere, compie scelte economiche; la libertà, la comprensibilità, l'effettiva volontà di quella scelta in termini economici è oggetto di analitica attenzione da parte del legislatore eurounitario (ad es., nella normativa consumeristica). Il legislatore richiede che il consumatore/interessato non solo voglia acconsentire (in termini classici diremmo: voglia l'atto), ma altresì che comprenda e voglia gli effetti giuridici di quel consenso (lo scambio, la concretizzazione degli impegni del fornitore, l'applicazione delle garanzie consumeristiche, ecc.). Solo così si può comprendere il tema della circolazione dei dati personali, e comprendere come esso sia divenuto ormai centrale nel fenomeno dell'economia digitale e realizzi una vicenda di circolazione della ricchezza.
E, del resto, non si può non dar conto che, con il recepimento della Direttiva n. 770/2019 sui contratti di fornitura di contenuto digitale e di servizi digitali nel nostro Codice del consumo, il legislatore italiano ha stabilito che la relativa disciplina si applica non solo ai contratti nei quali il consumatore acquista il bene o servizio pagando un prezzo monetario, ma altresì "nel caso in cui" il professionista fornisce o si obbliga a fornire un contenuto o servizio digitale al consumatore e il consumatore fornisce "o si obbliga a fornire dati personali" al professionista, escluse le ipotesi in cui tali dati siano trattati esclusivamente ai fini della fornitura del contenuto o servizio digitale oppure per assolvere a obblighi di legge del professionista e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti[23] (art. 135 *octies*, comma 4, D.Lg. n. 206/2005).

[23] Proprio questa 'esenzione' comprova che le ipotesi alle quali è estesa, alla circolazione del dato personale, la disciplina dei contratti con controprestazione monetaria, è solo ed esclusivamente quella nella quale sia rinvenibile una 'funzione' remuneratoria del dato personale e non anche, semplicemente, una – diversa – funzione attuativa di un programma contrattuale già posto. Il consenso al trattamento dei dati in funzione remunerativa, insomma, è prestato non solo in vista ed in occasione dell'ottenimento di un servizio o bene da parte del titolare (quale la possibilità di utilizzare una certa *app*, il diritto all'accesso e all'uso di un *social*, la possibilità di utilizzare un motore di ricerca, ecc.), ma un tale consenso al trattamento dei dati personali è prestato proprio in ragione dell'ottenimento di diritto all'uso di un servizio o di bene da parte del titolare e pertanto in una prospettiva di scambio: v., relativamente alla rilevanza del profilo funzionale, C. SOLINAS, *Autonomia privata*, cit., 89 ss.

La tecnica legislativa moderna normalmente non si impone all'attenzione degli interpreti per meditazione delle categorie e ponderazione della tecnica in relazione ai presupposti e agli obiettivi dell'intervento normativo, sicché non ci stupiamo del fatto che il legislatore italiano, in sede di recepimento, nulla abbia aggiunto al dettato europeo. Ha, però, modificato un termine ("obbligo" in luogo di "impegno") la cui portata, consapevole o meno che sia stata, attribuisce una sferzata verso il superamento definitivo della costruzione tradizionale del fenomeno in termini non patrimoniali. L'art. 135 *octies*, co. 4, Codice del consumo, contempla l'ipotesi in cui il consumatore "si obbliga" a fornire dati personali al professionista. L'adozione del concetto di obbligazione per qualificare l'impegno al conferimento del diritto a trattare i dati personali è certamente passaggio che tecnicamente ed etimologicamente vanifica quella 'neutralità' rispetto al fenomeno contrattuale che in sede europea si voleva fornire modificando l'originaria formulazione della proposta di direttiva.

In definitiva, il consenso al trattamento non può essere pensato asetticamente, senza alcuna valutazione del profilo funzionale all'operazione economica nella quale esso si inserisce.

Diversamente, non si comprenderebbe perché qualcuno debba prestare il proprio consenso al trattamento dei dati, se non per ottenere in cambio un servizio o un'utilità.

La prospettiva patrimonialistica non va temuta o avversata, ma la sua legittimazione concettuale – prima ancora che normativa –, una volta constatata senza pregiudizi, lascia, semmai, aperti numerosi problemi che meritano più consapevoli indagini. Tra questi, il problema del tipo contrattuale, il profilo funzionale dell'operazione, la natura onerosa o gratuita dei contratti dell'economia digitale, l'oggetto o le prestazioni dedotte in quello scambio, e così altri importanti profili che il fenomeno delle nuove tecnologie consegnerà al giurista nei prossimi anni.

CONSENSO AL TRATTAMENTO E LICEITÀ

Di Salvatore Orlando

SOMMARIO: 1. L'attualità del dibattito sul consenso privacy e sui suoi requisiti di libertà e consapevolezza. – 2. L'illiceità del trattamento dei dati personali per mancanza della base del consenso privacy in difetto di uno dei suoi requisiti di libertà, consapevolezza e manifestazione. – 3. La necessità di un dibattito sul requisito di liceità del consenso privacy. – 4. L'illiceità del trattamento dei dati personali per mancanza della base del consenso privacy in difetto del suo requisito di liceità laddove il consenso sia prestato per specifiche finalità di trattamento illegittime o il trattamento sia altrimenti vietato alla stregua di norme imperative del diritto unitario o nazionale (consenso illecito). – 5. Esempi - 5.1 Primo esempio: il consenso privacy esplicito illecito ex art. 9(2)(a) GDPR - 5.2 Secondo esempio: il divieto dell'art. 26(3) DSA. – 5.3 Terzo esempio: il divieto dell'art. 18(1)(c) del regolamento sul targeting della pubblicità politica. – 5.4 Quarto esempio: i divieti dell'art. 7 della direttiva sui lavoratori delle piattaforme online. – 5.5 Quinto esempio: i divieti di uso di sistemi di IA dell'art. 5 AI Act. – 5.6 Sesto esempio: lo sfruttamento delle vulnerabilità del Sig. Leon. – 5.7 Settimo esempio: la piattaforma illegale di concorsi a premi. – 5.8 Ottavo esempio: i divieti di trattamento della legge sull'oblio oncologico. – 5.9 Et cetera. – 6. L'invalidità del consenso privacy per illiceità è idonea a tutelare sia l'interessato che soggetti terzi. – 7. Tre aree di approfondimento. – 7.1 La finestra con vista fuori del GDPR (il test di legittimità delle finalità di trattamento non è solo endo-regolamentare). – 7.2 La questione della distribuzione di competenze tra autorità amministrative e giurisdizionali in relazione all'accertamento della legittimità/illegittimità delle finalità del trattamento. – 7.3 La ricerca della cassetta degli attrezzi più adeguata per affrontare le sfide ermeneutiche del consenso privacy nella data economy. – 8. Critica esemplare al Considerando 40 della direttiva sui lavoratori delle piattaforme online a dimostrazione della necessità di dismettere la concezione che si incentra esclusivamente sui requisiti di libertà e consapevolezza del consenso privacy. – 9. Critica esemplare alla formula definitoria del diritto all'oblio oncologico nella legge 193/2023 a dimostrazione della necessità di evidenziare la figura logica del divieto che caratterizza il contemporaneo diritto dei dati. – 10. Conclusioni sul consenso privacy come atto di autonomia privata e sulla prospettiva di una nuova stagione di studi sull'atto di autonomia privata di diritto unitario sollecitata dallo studio dell'illiceità del consenso privacy.

1. L'attualità del dibattito sul consenso privacy e sui suoi requisiti di libertà e consapevolezza.

La discussione sul consenso al trattamento dei dati personali (di seguito per brevità anche "consenso privacy") come base per il trattamento lecito dei dati personali ai sensi dell'art. 6(1)(a) del Regolamento (UE) 2016/679 (di seguito anche "GDPR" o il "Regolamento")[1] è

[1] Art. 6(1)(a) GDPR: "1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; (…)".

tornata di grande attualità dopo le numerose decisioni adottate dallo *European Data Protection Board* (di seguito anche "EDPB") e dalla Corte di giustizia dell'Unione Europea (di seguito anche "CGUE") in relazione a importanti tipologie di trattamenti di dati personali effettuati da società del gruppo Meta, con le quali, in sintesi, è stata ripetutamente negata la possibilità di utilizzare tanto la base dell'esecuzione del contratto quanto quella del legittimo interesse per i servizi Facebook, Instagram e WhatsApp[2], con ciò, sostanzialmente, indicandosi la necessità di ricorrere alla base del consenso; nonché dopo le prime contestazioni sulla liceità del trattamento di dati personali mosse ad OpenAI ai sensi del GDPR in relazione al servizio ChatGPT[3], e ai dubbi suscitati dalla spiegazione fornita dalla medesima società di ricorrere alla base del legittimo interesse per il trattamento di dati personali, da cui il recente rapporto della *task force* costituita *ad hoc* in seno all'EDPB per valutare la questione[4].

---

[2] Si fa riferimento innanzitutto alle tre decisioni vincolanti dello EDPB del 5 dicembre 2022 e ai successivi provvedimenti dell'autorità di controllo irlandese nei confronti di Meta del successivo 31 dicembre 2022 (per i servizi FB e Instagram) e di WhatsApp del gennaio del 2023, che hanno impedito a queste piattaforme di continuare ad utilizzare la base dell'esecuzione del contratto.
Successivamente, nell'ambito della controversia tra *Meta Platforms Inc*. e il *Bundeskartellamt* (l'autorità federale garante della concorrenza della Repubblica Federale di Germania) con sentenza del 4 luglio 2023, la CGUE ha dichiarato che l'articolo 6(1)(b) GDPR - che prevede la base giuridica dell'esecuzione di un contratto - debba essere interpretato nel senso che il trattamento di dati personali effettuato da Meta a proposito di Facebook, consistente nella profilazione a fini pubblicitari dell'utente, può essere considerato necessario per l'esecuzione di un contratto del quale gli interessati sono parti solo a condizione che detto trattamento sia oggettivamente indispensabile per realizzare una finalità che costituisce parte integrante della prestazione contrattuale destinata a quegli stessi utenti, cosicché l'oggetto principale del contratto non potrebbe essere conseguito in assenza di tale trattamento. In quella sentenza, la CGUE ulteriormente negato di per sé rilevanza al fatto che un simile trattamento dei dati personali sia menzionato nel contratto oppure che esso sia soltanto utile per la sua esecuzione. In particolare, secondo quanto si trova dichiarato dalla CGUE in quella sentenza, l'elemento determinante ai fini dell'applicazione della base giuridica del contratto è che il trattamento sia essenziale per consentire la corretta esecuzione del contratto stipulato tra quest'ultimo e l'interessato e che, pertanto, non esistano altre soluzioni percorribili e meno invasive. Quanto alla base giuridica del legittimo interesse, la CGUE dichiarava (sempre in quella sentenza) che la base prevista dall'art. 6(1)(f) GDPR può essere considerata idonea per la pubblicità profilata solo se: *(i)* il titolare del trattamento abbia precisamente informato gli interessati in merito al legittimo interesse; *(ii)* tale trattamento sia effettuato entro i limiti di quanto strettamente necessario alla realizzazione di suddetto interesse; e *(iii)* il contemperamento delle contrapposte pretese non comporti una prevalenza delle libertà e dei diritti fondamentali di tali utenti che richiedano la protezione dei dati personali sul legittimo interesse del titolare. Riferendosi al caso concreto che formava oggetto dei quesiti rivoltile in quel giudizio, la CGUE concludeva dichiarando che, in conseguenza di quanto sopra, né il contratto, né il legittimo interesse (né tantomeno l'obbligo legale o l'interesse vitale) potessero essere considerati basi giuridiche idonee ai fini della pubblicità personalizzata operata da Meta.
Ed infine il 27 ottobre 2023 l'EDPB ha emesso una decisione vincolante e urgente, la n. 1/2023, affinché l'autorità di controllo irlandese vieti definitivamente a Meta Ireland Limited di trattare i dati personali dei propri utenti per fini di pubblicità comportamentale sia sulla base del contratto che su quella del legittimo interesse: https://edpb.europa.eu/our-work-tools/our-documents/urgent-binding-decision-board-art-66/urgent-binding-decision-012023_en.

[3] Ci riferiamo innanzitutto al provvedimento cautelare della nostra Autorità garante per la protezione dei dati personali (di seguito anche il "Garante privacy italiano") del 30 marzo 2023, alla successiva misura di sospensione condizionata del medesimo provvedimento dell'11 aprile 2023 e all'atto di contestazione di violazione della normativa in materia di protezione dei dati personali relativamente al servizio ChatGPT che il Garante privacy italiano ha notificato a OpenAI LLC e ha comunicato al pubblico il 29 gennaio 2024. Nel comunicato, il Garante specificava che la misura segue il provvedimento adottato dalla medesima Autorità il 30 marzo 2023, e che l'istruttoria svolta ha fatto emergere elementi che possono configurare una o più violazioni delle disposizioni del GDPR (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9978020).

[4] Il report del 23 maggio 2024 evidenzia una serie di criticità del servizio ChatGPT circa il rispetto delle prescrizioni del GDPR, toccando i temi della liceità del trattamento (in particolare sottolineando la necessità che ricorra una delle basi previste dal primo paragrafo dell'art. 6 del Regolamento e prendendo in considerazione le diverse fasi e attività implicate dal servizio, quali la raccolta, compreso il *web scraping*, la preelaborazione e l'addestramento dei dati, nonché le attività e fasi di *input*, *prompt* e *output*) della correttezza, della trasparenza e

Di grande attualità è in particolare il tema dei requisiti del consenso privacy, *in primis* quelli che attengono alla consapevolezza e alla libertà dell'interessato, che, come risaputo, devono ricorrere per la prestazione di un consenso valido, ai sensi dell'art. 4, n. 11) del Regolamento[5]. Tale tema, già centrale nel dibattito sul c.d. *tying*[6], ha ricevuto di recente un nuovo impulso a proposito della diffusione delle formule c.d. *Pay or Ok* (note anche come "*Consent or Pay*", o "acconsenti o paga"). Esse, implementate a partire dal 2022 da alcune testate giornalistiche

degli obblighi di informazione, dell'accuratezza e dei diritti degli interessati (https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf).

[5] Art. 4, n. 11), GDPR "«consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento".

[6] Espressione con la quale si fa riferimento all'eventualità, considerata nell'art. 7, § 4, GDPR, 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. I Considerando 42 e 43 del GDPR chiaramente collegano questa disposizione al requisito di libertà del consenso *privacy*. Limitandoci ad alcuni dei contributi più recenti (ai quali si rinvia anche per riferimenti più completi alla dottrina precedente e alla giurisprudenza rilevante) cfr.: P. STANZIONE, *La libertà e il suo valore*¸ in *Commerciabilità dei dati personali. Profili economici, giuridici, etici della monetizzazione*, a cura di G. Cerrina Feroni, Bologna, 2024, 149 ss.; G. FINOCCHIARO, *Consenso al trattamento e libertà*, in *Pers. merc.*, 2024, 3 ss.; V. RICCIUTO, *Consenso al trattamento e contratto*, in *Pers. merc.*, 2024, 14 ss., spec. 22 ss.; ID., *L'equivoco della privacy. Persona vs dato personale*, Napoli, 2022; G. SCORZA, *La deducibilità nell'oggetto del contratto del diritto a trattare i dati personali*, in *Commerciabilità dei dati personali*, cit., 231 ss., spec. 245 ss.; C.A. TROVATO, Everything has its price? *Una riflessione sulle pratiche di commercializzazione dei dati* personali, ivi, 301 s.; E. TOSI, *Dati personali e contratto: un ossimoro apparente*, in *European Journal of Privacy Law & Technologies*, 2023/2, 79 ss.; ID., *Circolazione contrattuale dei dati personali tra contratto e responsabilità,* Milano, 2023; F.A. GENOVESE, *Trattamento dei dati personali e consenso dell'interessato*, in *La circolazione dei dati personali: persona, contratto e mercato*, a cura di A. Morace Pinelli, Pisa, 2023, 93 ss.; A. GENTILI, *La volontà nel contesto digitale: interessi del mercato e diritti delle persone*, in *Riv., trim. dir. proc. civ.*, 2022, 711 ss.; S. ORLANDO, *Il coordinamento tra la direttiva 2019/770 e il GDPR. L'interessato-consumatore*, in *Pers. merc.*, 2023, 230 ss., e in *Commerciabilità dei dati personali*, cit., 157 ss.; ID., *Per un sindacato di liceità del consenso privacy*, in *Pers. merc.*, 2022, 528 ss.; F. CAGGIA, *Cessione di dati personali per accedere al servizio digitale gratuito: il modello del "consenso rafforzato"*, in *I problemi dell'informazione nel diritto civile, oggi. Studi in onore di Vincenzo Cuffaro*, Roma, 2022, 417 ss; L. CASALINI, *Dati e identità personale. Note sparse a partire da una recente pronuncia del Consiglio di Stato*, in *Annuario 2022 Osservatorio Giuridico sull'Innovazione Digitale*, a cura di S. Orlando e G. Capaldo, Roma, 2022, 53 ss.; A. DE FRANCESCHI, *Personal data as Counter-Performance*, in *Privacy and Data Protection in Software Services*, a cura di R. Senigaglia, C. Irti e A. Bernes, Singapore, Springer, 2022, 59 ss.; ID, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, 67 ss.; P. HACKER, *Regulating the economic impact of data as counter-performance: from the illegality doctrine to the unfair contract terms directive*, in *Data as counter-performance – Contract law 2.0?* a cura di S. Lohsse, R. Schulze e D. Staudenmayer, Bloomsbury Publishing, Londra, 2020, 47 ss.; V. JANEˇCEK e G. MALGIERI, *Data extra commercium*, ivi, 95 ss.; S. LOHSSE, R. SCHULZE, D. STAUDENMAYER, *Data as counterperformance – contract law 2.0? An introduction*¸ ivi, 9 ss.; A. METZGER, *A market model for personal data: state of play under the new directive on digital content and digital services*, ivi. cit., 25 ss.; S. VAN ERP, *Management as ownership of data*, ivi, 77 ss.; C. WENDEHORST, *Personal data in data value chains – is data protection law fit for the data economy?,* ivi, 193 ss.; C. SOLINAS, *Autonomia privata e regolazione pubblica nel trattamento dei dati personali*, Bari, 2022; A.M. GAMBINO e A. STAZI, *Introduzione. Datificazione dei rapporti socio-economici, circolazione dei dati e diritto*, in *La circolazione dei dati*, a cura di A.M. Gambino e A. Stazi, Pisa, Pacini, 2020, XI; G. MARCHETTI e S. THOBANI, *La tutela contrattuale dei consumatori di contenuti e servizi digitali*, in *Manuale di diritto privato delle nuove tecnologie* a cura di G. Magri, S. Martinelli e S. Thobani, Torino, 2022, 35 ss., spec. 46 ss.; G. D'IPPOLITO, *Monetizzazione, patrimonializzazione e trattamento dei dati personali*, in *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, a cura di E. Cremona, F. Laviola e V. Pagnanelli, Torino, 2022, 51 ss. Per i problemi generali interessati dalla tematica della libertà del consenso nell'ecosistema digitale, cfr. anche i contributi di C. CAMARDI, *Dalla logica individualistica alla regolazione della complessità nella tutela del consumatore (e delle vulnerabilità) nell'ecosistema digitale*, in *Mercato digitale e tutela dei consumatori. Prove di futuro*, a cura di G. Grisi e S. Tommasi, Torino, 2023, 217 ss.; A. MORACE PINELLI, *Introduzione*, in *La circolazione dei dati personali: persona, contratto e mercato*, cit., 11 ss.

online[7], si sono recentemente diffuse presso Facebook e altre piattaforme, che hanno inteso così adeguarsi all'indicazione circa la doverosità della base del consenso, espressa nei predetti provvedimenti riguardanti i servizi di Meta.
Sul punto – alimentando ulteriormente il dibattito – è intervenuto da ultimo il parere dell'EDPB 8/2024[8]. In esso, l'EDPB ha esaminato la compatibilità della formula acconsenti o paga con il requisito di libertà del consenso, limitatamente, tuttavia, alle "piattaforme online di grandi dimensioni", una categoria - dobbiamo sottolinearlo - disegnata *ad hoc* dall'EDPB ai fini del medesimo parere, e che non ha un riscontro normativo. Facendo ciò, l'EDPB ha dichiaratamente escluso dal suo parere i trattamenti di dati personali operati da titolari diversi dalle "piattaforme online di grandi dimensioni", tra cui anche - così sembra doversi ritenere - le testate giornalistiche online che hanno per prime diffuso la formula *Pay or Ok*.
Nell'ambito tematico dei requisiti di consapevolezza e libertà del consenso privacy deve inquadrarsi anche la crescente attenzione riservata al *consenso al trattamento dei dati personali ottenuto in modo sleale, ossia falsato da comportamenti scorretti sulle interfacce online*. È il fenomeno noto con l'espressione "*dark patterns*", più di recente sostituita da quella "*deceptive design patterns*" [9].
Con queste espressioni si individuano certe caratteristiche fuorvianti delle interfacce online, ossia dei software che governano l'esperienza degli utenti online[10]. Il fenomeno riguarda il disegno di questi software, che può essere piegato a fini di distorsione del comportamento degli utenti online. Esso non riguarda, dunque, soltanto la distorsione del consenso privacy, concernendo qualsiasi comportamento dell'utente online. Naturalmente, però, poiché questo fenomeno investe anche e massicciamente l'influenza sulla prestazione del consenso privacy, di esso si è interessato l'EDPB, che ha emanato delle apposite Linee guida (la prima versione era intitolata ai *dark patterns*; quella più recente del febbraio 2023, la versione 2.0, è intitolata ai *deceptive design patterns*, ossia, come detto, la nuova espressione per indicare lo stesso fenomeno)[11]; e il Garante privacy italiano ha pubblicato sul suo sito internet una pagina informativa[12].
A questo fenomeno sono dedicati segnatamente il Considerando 67 e l'art. 25 del *Digital Services Act* (il regolamento (UE) 2022/2065, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE, innanzi anche "DSA").
Il tema si intreccia con quello della disciplina delle pratiche commerciali scorrette, di cui alla direttiva 2005/29/CE (innanzi anche "UCPD"), rendendo necessario instaurare ermeneuticamente il giusto rapporto tra questi tre plessi normativi (UCPD, GDPR e DSA)[13].

---

[7] V. i comunicati del Garante privacy italiano del 18.10.2022 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9815415), del 21.10.2022 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9816536) e del 12.11.2022 (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9822601) di avvio di istruttorie a carico di testate editoriali online. In dottrina, v. R. MONTINARO, *I* cookie paywall *e le testate giornalistiche* online*: si tratta di un "consenti a tutto o paga"?*, in *Mercato digitale e tutela dei consumatori*, cit., 187 ss.
[8] Parere 8/2024 dell'EDPB del 17 aprile 2024: https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf
[9] Cfr. S. ORLANDO, *A proposito dei deceptive design (già dark) patterns*, in *Mercato digitale e tutela dei consumatori*, cit., 63 ss.
[10] La definizione di interfaccia online è contenuta all'art. 3, lett. *m)*, DSA: "«interfaccia online»: qualsiasi software, compresi i siti web o parti di essi, e le applicazioni, incluse le applicazioni mobili".
[11] https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf
[12] https://www.garanteprivacy.it/temi/internet-e-nuove-tecnologie/dark-pattern
[13] Non possiamo soffermarci qui su questo aspetto, che richiederebbe una trattazione *ad hoc*. Per un primo orientamento, v. S. ORLANDO, *A proposito dei deceptive design (già dark) patterns*, cit., spec. 98 ss. e 106 s. Il tema del rapporto tra fonti nel diritto dei dati non si esaurisce, naturalmente, all'ambito delle fonti che rispondono al principio del divieto dello sfruttamento delle vulnerabilità decisionali delle persone fisiche (di cui è espressione

Infine, e naturalmente, nel dibattito sul ruolo del consenso privacy come base del trattamento dei dati personali, risulta centrale – e, per essere franchi: ancora tutta da centrare – l'analisi delle recenti e numerose normative che hanno contrattualizzato o preso atto della contrattualizzazione[14] di una pluralità di rapporti che comportano la disposizione e il trattamento di dati personali su base volontaria.

la disciplina di contrasto dei c.d. *deceptive design patterns*), ma investe ogni altro ambito del diritto dei dati nel quale possano ravvisarsi principî comuni a più fonti. Per fare un esempio, è questo l'ambito del contrasto alla discriminazione, dove pure si pongono problemi di coordinamento tra varie fonti del diritto dei dati (cfr. per tutti, S. TOMMASI, *The Risk of Discrimination in the Digital Market. From the Digital Services Act to the Future*, Springer, Londra, 2023).

[14] Come noto, il dibattito sulla contrattualizzazione dei rapporti che comportano il trattamento dei dati personali è molto acceso. Per un'analisi ragionata ed aggiornata delle diverse posizioni, ed i relativi riferimenti bibliografici, v. per tutti V. RICCIUTO, *Consenso al trattamento e contratto*, cit., 14 ss.

Si fa riferimento alla *Digital Content Directive* (di seguito anche "DCD")[15], alla direttiva *Omnibus*[16], al *Data Governance Act* (di seguito anche "DGA")[17], al DSA[18], al *Data Act*[19].
Mentre in tutte queste fonti è dichiarata e ribadita la prevalenza del GDPR, risulta ancora mancante in dottrina, presso i giuristi europei, un disegno teorico organico idoneo a legare tutte queste normative in una trama concettuale unitaria, coerente e sufficientemente condivisa, che vada al di là della, pacifica, dichiarazione della prevalenza del GDPR. In questo contesto, e nel difetto di una teoria unitaria, quella dichiarazione rischia effettivamente di diventare una formula declamatoria vuota o imperfetta; inidonea, cioè, ad orientare efficacemente

[15] Direttiva (UE) 2019/770 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali. Viene in particolare in rilievo la seguente proposizione dell'art. 3(1) DCD: "(…) La presente direttiva si applica altresì nel caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore *e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico*, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dall'operatore economico ai fini della fornitura del contenuto digitale o del servizio digitale a norma della presente direttiva o per consentire l'assolvimento degli obblighi di legge cui è soggetto l'operatore economico e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti".

[16] Direttiva (UE) 2019/2161 che modifica la direttiva 93/13/CEE e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori. In particolare, viene in rilievo l'art. dall'art. 4, punto 2), lett. b) della direttiva *Omnibus*, che ha inserito l'art. 1 *bis* Direttiva 2011/83/UE contenente una disposizione conforme a quella sopra riportata dell'art. 3(1) DCD: "1-*bis*. La presente direttiva si applica anche se il professionista fornisce o si impegna a fornire un contenuto digitale mediante un supporto non materiale o un servizio digitale al consumatore *e il consumatore fornisce o si impegna a fornire dati personali al professionista*, tranne i casi in cui i dati personali forniti dal consumatore siano trattati dal professionista esclusivamente ai fini della fornitura del contenuto digitale su supporto non materiale o del servizio digitale a norma della presente direttiva o per consentire l'assolvimento degli obblighi di legge cui il professionista è soggetto, e questi non tratti tali dati per nessun altro scopo" (corsivo nostro).

[17] Regolamento (UE) 2022/868 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724. Del DGA vengono in rilievo la disciplina sull'"intermediazione dei dati" (Capo III artt. 10-15 DGA) e quella sull'«altruismo dei dati» (Capo IV, artt. 16-25 DGA), che riguardano entrambe tanto dati non personali che dati personali e che prevedono chiaramente titoli e rapporti contrattuali per la condivisione dei dati, come ivi prevista e definita. Il servizio di intermediazione di dati è definito come quel servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro 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, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali (art. 2, n. 11 DGA). Ai fini di questa definizione e di quella sull'altruismo dei dati, il DGA definisce la "condivisione dei dati" come la fornitura di dati da un interessato o un titolare dei dati a un utente dei dati ai fini dell'utilizzo congiunto o individuale di tali dati, *sulla base di accordi volontari o del diritto dell'Unione o nazionale, direttamente o tramite un intermediario, ad esempio nel quadro di licenze aperte o commerciali, dietro compenso o a titolo gratuito* (art. 2, n. 10 DGA). L'altruismo dei dati è definito come la condivisione volontaria di dati sulla base del *consenso accordato dagli interessati al trattamento dei dati personali* che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, *senza la richiesta o la ricezione di un compenso* che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale (art. 2, n. 16 DGA).

[18] Del DSA vengono in rilievo le norme che prevedono che i destinatari dei servizi di piattaforme online possano modificare i parametri della pubblicità ad essi rivolta (art. 26 DSA) e le opzioni che influenzano i parametri dei sistemi di raccomandazione che determinano l'ordine delle informazioni ad essi presentate (art. 27 DSA).

[19] Regolamento (UE) 2023/2854 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828. Del *Data Act* vengono in rilievo la disciplina della condivisione su base contrattuale dei dati da impresa a consumatore e da impresa a impresa, compresa la condivisione dei dati generati dall'uso di prodotti connessi e dei servizi correlati, come ivi definiti (Capi II e III, artt. 3-12 *Data Act*) e quella delle clausole abusive nei contratti tra imprese che hanno ad oggetto l'accesso e l'utilizzo di dati (Capo IV, art. 13 *Data Act*).

l'interpretazione e l'applicazione delle norme nella ricerca di soluzione ai molti problemi applicativi che già si intravedono.

2. L'illiceità del trattamento dei dati personali per mancanza della base del consenso privacy in difetto di uno dei suoi requisiti di libertà, consapevolezza e manifestazione

Come noto, al principio di liceità del trattamento dei dati personali, enunciato all'art. 5(1)(a) del Regolamento[20], secondo cui i dati personali devono essere trattati in modo lecito (oltre che corretto e trasparente nei confronti dell'interessato), segue la disposizione del § 1 dell'art. 6 GDPR, a tenore del quale il trattamento è lecito solo se e nella misura in cui ricorra una delle condizioni previste nelle lettere da a) a f) del medesimo paragrafo: le cosiddette 'basi' del trattamento.
Il modo tradizionale di affrontare il problema della liceità a proposito del trattamento dei dati personali segue questa scansione normativa.
Pertanto, quando viene in questione la ricorrenza della base del consenso *privacy*, si dice che il trattamento dei dati personali è lecito se l'interessato abbia prestato un consenso che abbia tutti i requisiti previsti per il consenso dall'art. 4, n. 11), GDPR: una manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento[21].
Sono le condizioni che in breve possiamo chiamare come requisiti di libertà, consapevolezza e manifestazione del consenso *privacy*.
Ogni dichiarazione dell'interessato prestata senza i prescritti requisiti di libertà, consapevolezza e manifestazione previsti dal GDPR per il consenso privacy si intende prestata "in violazione" del Regolamento, e dunque "non è vincolante" come consenso (arg. art. 7, § 2, ultima proposizione, GDPR).
Questo sta anche a significare che quando ci si riferisce alle condizioni appena richiamate di libertà, consapevolezza e manifestazione del consenso, *il loro difetto comporta l'illiceità del trattamento* dei dati personali *ex* art. 5, § 1, lett. a) del Regolamento, in quanto il consenso, non avendo una di quelle condizioni o requisiti, non è vincolante come tale, e dunque viene a mancare la necessaria 'base' per un trattamento lecito dei dati personali.
Rivolgendoci ora alle tipologie problematiche di condizionamento del consenso *privacy* richiamate dianzi, che – come abbiamo detto (v. par. 1 *supra*) – occupano attualmente in misura quasi esclusiva il dibattito sul consenso *privacy*, ossia ai fenomeni dei *dark* o *deceptive design patterns*, del *tying*, e delle formule *Pay or Ok* , possiamo dire conclusivamente che ad essere in gioco per ciascuno di tali fenomeni sono la liceità/illiceità del *trattamento* a seconda della ricorrenza/mancanza dei requisiti di libertà e consapevolezza del *consenso privacy*.
Così, in particolare, quando il consenso *privacy* è falsato dalle interfacce attraverso "percorsi oscuri" o "modelli fuorvianti", sarà corretto parlare di illiceità del *trattamento* per difetto di un consenso vincolante come tale, perché il consenso ottenuto dal titolare in quel modo difetta delle condizioni di consapevolezza, e talvolta anche della condizione di libertà, prescritte dal Regolamento, e dunque non è valido e vincolante come consenso ai sensi del GDPR come base di un trattamento lecito. Allo stesso modo, le indagini sui requisiti del consenso privacy svolte a proposito del *tying* e delle formule "acconsenti o paga" riguardano le alternative, di cui

[20] Art. 5, § 1, lett. a), GDPR: "1. I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); (…)".
[21] V. *ex multis*, F.A. GENOVESE, *Trattamento dei dati personali e consenso dell'interessato*, cit., spec. p 91 ss.

dispone in concreto l'interessato, in quanto ritenute rilevanti per asseverare la sua effettiva libertà e talvolta anche la sua effettiva consapevolezza nel prestare il consenso *privacy*. Con la conseguenza che dovrà ritenersi il consenso *privacy* invalido per difetto di quei requisiti e il relativo trattamento dei dati personali illecito tutte le volte in cui le indagini condotte in concreto portino alla conclusione dell'assenza in concreto dei requisiti di libertà e/o consapevolezza.

3. La necessità di un dibattito sul requisito di liceità del consenso *privacy*

Salvo che per alcune sollecitazioni[22], non sembra invece essersi ancora sviluppato un dibattito su un requisito del consenso privacy per così dire implicito, ossia non espressamente contemplato dalla lettera del GDPR: il requisito della liceità del consenso *privacy*.
Intendo qui riferirmi ad un requisito *ulteriore e autonomo* rispetto a quelli di libertà, consapevolezza e manifestazione, sopra ricordati. Per chiarezza, chiamerò nel prosieguo del presente contributo il consenso privacy che difetti del requisito di liceità - nel senso specifico che proverò di seguito ad esporre - come consenso *privacy illecito*. Devo però al contempo segnalare, in proposito, che in letteratura e in alcuni provvedimenti del Garante *privacy* italiano, si utilizza talvolta l'espressione 'consenso illecito' per far riferimento proprio al consenso *privacy* che difetta dei requisiti di libertà, consapevolezza e manifestazione previsti espressamente dal GDPR e ricavati dalla definizione di consenso ex art. 4, n. 11 del Regolamento[23]. Spero di riuscire ad esporre in modo convincente nel presente saggio i motivi per i quali ritengo invece corretto e utile individuare e indicare con il concetto di 'illiceità' un distinto spazio di trattamento e di valutazione normativa del consenso *privacy*.
Il requisito di liceità del consenso *privacy*, inteso in questa accezione autonoma dai requisiti ricavati dall'art. 4, n. 11, GDPR deve, a mio avviso, delinearsi sulla base del combinato disposto delle previsioni dell'art. 5, § 1, lett. b), GDPR, nella parte in cui prescrive che i dati personali debbano essere "raccolti per finalità […] *legittime*"[24], e dell'art. 6, §1, lett. a), GDPR. Quest'ultima disposizione va coordinata con la prima nel senso che deve essere aggiunto in via interpretativa l'aggettivo "legittime" al sostantivo "finalità" ivi utilizzato, così che la relativa

---

[22] Cfr. P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, in *Diritto alla riservatezza e circolazione dei dati personali*, a cura di R. Pardolesi, Milano, 2003, 395, spec. p 412-413 e 415; S. ORLANDO, *Per un sindacato di liceità del consenso privacy*, in *Pers. merc.* 2022, 527 ss.; D. IMBRUGLIA, *Le presunzioni delle macchine e il consenso dell'interessato*, in *Riv. trim. dir. proc. civ.*, 2023, 921 ss., spec. p 944-945; G. VETTORI, *Rodolfo Sacco e la civilistica del XXI secolo*, in *Esperienze giuridiche in dialogo. Il ruolo della comparazione*, a cura di M. Graziadei e A. Somma, Roma, 2024, 143, e in *Riv. trim. dir. proc. civ.*, 2023, 539 ss.
[23] Cfr. per tutti G. SCORZA, *La deducibilità nell'oggetto del contratto del diritto a trattare i dati personali*, cit., 245 ss. Per i provvedimenti del Garante *privacy* italiano, v. quello del 23 febbraio 2023 nei confronti di Ediscom S.A. nel quale si legge il seguente passaggio: "In conclusione si è ritenuto che, un consenso raccolto con tali modalità, volutamente progettate per eludere le norme, destasse molte perplessità in ordine alla libertà e alla consapevolezza con cui l'interessato può esprimere la propria volontà e pertanto non poteva essere considerato lecito" (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870014).
[24] Art. 5, § 1, lett. b), GDPR: "I dati personali sono: (…) b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); (…)". Che la determinata finalità del trattamento per la quale l'interessato acconsente al trattamento debba essere «legittima» è previsto espressamente anche nel nuovo regime dell'altruismo dei dati predisposto dal *Data Governance Act*. V. art. 21, § 1, lett. a), DGA: "1. Un'organizzazione per l'altruismo dei dati riconosciuta informa in maniera chiara e facilmente comprensibile gli interessati o i titolari dei dati, prima di qualsiasi trattamento dei loro dati, in merito: a) agli obiettivi di interesse generale e, se opportuno, alla finalità determinata, esplicita e legittima per cui i dati devono essere trattati, e per i quali acconsentono al trattamento dei loro dati da parte di un utente dei dati".

condizione dell'art. 6, § 1, lett. a), GDPR deve essere letta come se recitasse: "l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità *legittime*".
Una simile lettura non sembra possa essere messa in dubbio, essendo assolutamente pacifico che i principî di cui all'art. 5 GDPR trovino applicazione con riferimento a ciascuna e a tutte le condizioni per il trattamento lecito, di cui al successivo art. 6.
Non vedendosi d'altronde come potrebbe sostenersi che costituisca una base di lecito trattamento dei dati personali quella per cui l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità *illegittime*, deve senz'altro concludersi che l'aggettivo "legittime" è sottinteso nella lettera a) del primo paragrafo dell'art. 6 del Regolamento.
Se si conviene con quanto sopra, si dovrà anche riconoscere – già in astratto – la possibilità che le specifiche finalità di trattamento per le quale il titolare del trattamento chiede e ottiene il consenso dall'interessato, possano essere illegittime. Ed invero, come il Regolamento implicitamente prevede che esse *debbano* essere legittime, si dovrà convenire che il medesimo Regolamento implicitamente preveda che esse *possano* essere illegittime.
Ed è questo appunto il campo per il sindacato della liceità del consenso *privacy*, di cui sembra corretto debba affacciarsi la necessità di un dibattito. Quelle norme, in altre parole, consentono uno specifico sindacato di liceità del consenso *privacy* (ulteriore e diverso rispetto a quello che riguarda i requisiti di libertà, consapevolezza e manifestazione, fissati dall'art. 4, n. 11, GDPR), ma al contempo lo impongono, perché impongono di considerare l'ipotesi che le specifiche finalità del trattamento dei dati personali per cui l'interessato presta il consenso *privacy* siano illegittime.
Per lo stesso motivo, e in via più generale, non sembra possa negarsi nemmeno in linea teorica che debba considerarsi invalido un consenso privacy reso da un interessato a fronte di *un divieto legale posto al titolare del trattamento di raccogliere i dati personali che formano oggetto di quel consenso privacy*. Come vedremo più avanti, i divieti di questo tipo sono variamente articolati (par. 4 *infra*), e numerosi sono gli esempi che possono farsi al riguardo (par. 5 *infra*). Essi confluiscono tutti nell'ambito tematico del dibattito che sembra necessario promuovere sulla liceità del consenso privacy.

4. L'illiceità del trattamento dei dati personali per mancanza della base del consenso privacy in difetto del suo requisito di liceità laddove il consenso sia prestato per specifiche finalità di trattamento illegittime o il trattamento sia altrimenti vietato alla stregua di norme imperative del diritto unitario o nazionale (consenso illecito).

Alla luce delle considerazioni svolte nel par. 3 *supra*, sembra corretto postulare un requisito di liceità del consenso *privacy* diverso dai requisiti di libertà, consapevolezza e manifestazione del consenso *privacy*.
Sembra ulteriormente corretto ritenere che, similmente a quanto accade per il difetto dei requisiti di libertà, consapevolezza e manifestazione del consenso *privacy*, debba dirsi che anche nel caso di difetto del requisito di liceità del consenso privacy (inteso nel senso detto), il trattamento dei dati personali dovrà ritenersi illecito.
Ciò in quanto, anche in questo caso, dovrà dirsi che una dichiarazione dell'interessato prestata per acconsentire al trattamento di propri dati personali per finalità *illegittime*, in contrasto con la prescrizione dell'art. 5, §1, lett. b), GDPR, costituisce una "violazione" del Regolamento e come tale non è "vincolante" (arg. art. 7, § 2, ultima proposizione, GDPR). E cioè che essa non è vincolante come consenso *privacy*.

Pertanto qualsiasi dichiarazione di consenso al trattamento dei dati personali prestata per una o più specifiche finalità di trattamento illegittime non può costituire una valida base per il trattamento dei dati personali.
In questo senso, potrà sinteticamente dirsi anche che l'illiceità del consenso *privacy* (nello specifico senso qui esposto) comporta l'illiceità del relativo trattamento dei dati personali, ossia del trattamento dei dati personali che voglia basarsi sul consenso *privacy* illecito.
Se si conviene con quanto sopra, dovrà ora anche convenirsi sul fatto che la rilevanza della legittimità delle finalità del trattamento ai fini del giudizio sulla validità del consenso *privacy* consente ed impone di ritenere rilevanti i divieti legali di trattamento di dati personali.
Come esporrò nel successivo paragrafo dedicato agli esempi (v. par. 5 *infra*), divieti di questo tipo sono sempre più numerosi a cospetto della definitiva affermazione della *data economy*, e della conseguente esigenza, sempre più avvertita dal legislatore europeo e dai legislatori nazionali, di porre dei limiti legali all'industria dei dati.
Tali divieti si presentano come variamente articolati, prevedendo e combinando insieme in modi di volta in volta diversi (in relazione alle diverse finalità disciplinari assolte dai divieti) gli elementi rilevanti per la fattispecie del divieto, e così disegnando variamente quelli relativi ai destinatari del divieto (generalità dei titolari o determinate categorie di titolari del trattamento dei dati) ai dati personali che formano l'oggetto del trattamento vietato (generalità dei dati personali o determinate categorie di dati personali) e alle finalità del trattamento (qualsiasi finalità o determinate categorie di finalità), nonché inserendo la previsione di altre circostanze fattuali variamente qualificate, anche temporalmente.
Potranno dunque definirsi invalidi in quanto illeciti, tanto i consensi *privacy* prestati a fronte di specifici divieti posti a determinate categorie di titolari di trattare determinate categorie di dati personali per determinate finalità (ove il consenso *privacy* riguardi dati personali rispondenti a quelle determinate categorie e sia prestato per quelle determinate finalità vietate), quanto i consensi *privacy* prestati a fronte di specifici divieti rivolti alla generalità dei titolari di trattare determinate categorie di dati per qualsivoglia finalità, eccezion fatta solo per determinate finalità (ove il consenso *privacy* riguardi quelle determinate categorie di dati e sia prestato per finalità diverse da quelle eccezionalmente ammesse), quanto i consensi *privacy* prestati a fronte di specifici divieti di trattamento di determinate categorie di dati personali per certe finalità al di fuori di determinate circostanze fattuali e limiti temporali, che comportano, di converso, l'autorizzazione al trattamento solo entro certi limiti fattuali, ivi compresi certi limiti temporali.

5. Esempi.

5.1. Primo esempio: il consenso privacy esplicito illecito ex art. 9(2)(a) GDPR

L'art. 9, § 2, lett. a), GDPR prevede espressamente un esempio normativo di consenso *privacy* illecito, nel senso inteso nel presente scritto.
Come noto, il divieto del trattamento delle particolari categorie di dati di cui al § 1 dell'art. 9 GDPR può essere superato soltanto a certe condizioni, ossia su certe basi, tra cui quella del consenso "esplicito". Come pure noto, tuttavia, l'art. 9, § 2, lett. a) aggiunge che tale consenso *privacy* esplicito non può valere a superare il divieto di cui al §1 del medesimo articolo *laddove ciò non sia consentito alla stregua del diritto dell'Unione o del diritto nazionale applicabile*[25].

[25] Il § 1 e il § 2, lett. a) dell'art. 9 GDPR, rubricato "Trattamento di categorie particolari di dati personali» così recano: "1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi

Ciò sta a significare che in costanza di una norma imperativa esterna al Regolamento, di diritto unitario o nazionale, che vieta il trattamento di quei dati personali in modo inderogabile, il consenso *privacy* è invalido in quanto illecito, con la conseguenza che ogni relativo trattamento sarebbe illecito.
È una manifestazione normativa della illiceità del consenso *privacy* di cui vado parlando.

5.2. Secondo esempio: il divieto dell'art. 26(3) DSA

L'art. 26, § 3, DSA prevede che i fornitori di piattaforme *online* non possono presentare pubblicità ai destinatari del servizio basate sulla profilazione (come definita nel GDPR) utilizzando le categorie speciali di dati personali di cui all'articolo 9, § 1, GDPR.
Tale norma prevede dunque uno specifico divieto di trattamento di una determinata categoria di dati personali per una determinata finalità rivolto a determinati destinatari, tale per cui debbono ritenersi invalidi in quanto illeciti i consensi *privacy* che siano prestati per questo trattamento vietato.

5.3. Terzo esempio: il divieto dell'art. 18(1)(c) del regolamento sul targeting della pubblicità politica

Similmente, l'art. 18, § 1, lett. c) del recente regolamento (UE) 2024/900 sulla trasparenza e il targeting della pubblicità politica[26] vieta le tecniche di *targeting* o di consegna del messaggio pubblicitario in ambito di pubblicità politica *online* che si avvalgano di tecniche di profilazione (come definita nel GDPR) utilizzando le categorie speciali di dati personali di cui all'articolo 9, § 1, GDPR.
Anche in questo caso dovremo dire che siamo in presenza di una norma che prevede uno specifico divieto di trattamento di una determinata categoria di dati personali per una determinata finalità, tale per cui devono ritenersi invalidi in quanto illeciti i consensi *privacy* che siano prestati per questo trattamento vietato.

5.4. Quarto esempio: i divieti dell'art. 7 della direttiva sui lavoratori delle piattaforme online

L'art. 7 della direttiva, recentemente adottata, relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali[27], *inter alia* vieta alle piattaforme di lavoro digitali (come ivi definite) di trattare mediante sistemi decisionali o di monitoraggio automatizzati (come ivi definiti): (a) dati personali relativi allo stato emotivo o psicologico della persona che svolge un lavoro mediante piattaforme digitali; (b) dati personali relativi a

---

a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. 2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, *salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1*; (…)".

[26] Regolamento (UE) 2024/900 del 13 marzo 2024 relativo alla trasparenza e al *targeting* della pubblicità politica.

[27] Si fa riferimento al testo della direttiva adottato dal Parlamento europeo e dal Consiglio dell'Unione europea, ma non ancora pubblicato sulla GU dell'UE alla data in cui il presente saggio è stato inviato per la pubblicazione (https://www.europarl.europa.eu/news/it/press-room/20240419IPR20584/riders-il-parlamento-adotta-la-direttiva-sul-lavoro-delle-piattaforme).

conversazioni private; (c) dati personali quando la persona che svolge un lavoro mediante piattaforme digitali non sta svolgendo un lavoro mediante le stesse o non si sta offrendo per svolgerlo; (d) dati personali per prevedere l'esercizio di diritti fondamentali, compresi il diritto di associazione, il diritto di negoziazione e di azioni collettive o il diritto all'informazione e alla consultazione, quali definiti nella Carta dei diritti fondamentali della Unione europea; (e) dati personali per desumere l'origine razziale o etnica, lo status di migrante, le opinioni politiche, le convinzioni religiose o filosofiche, la disabilità, lo stato di salute, comprese le malattie croniche o la sieropositività, lo stato emotivo o psicologico, l'adesione a un sindacato, la vita sessuale o l'orientamento sessuale di una persona; (f) i dati biometrici, come definiti nel GDPR, di una persona che svolge un lavoro mediante piattaforme digitali per stabilirne l'identità confrontandoli con i dati biometrici di persone memorizzati in una banca dati.
Anche in questo caso siamo in presenza di una disciplina che prevede specifici divieti di trattamento di dati personali, e tali divieti sono variamente articolati non soltanto relativamente alle categorie di dati personali ma anche relativamente alle finalità e alle circostanze fattuali del trattamento (v. par. 4 *supra*). Anche in questo caso devono ritenersi invalidi in quanto illeciti i consensi privacy che siano prestati per i trattamenti vietati.

5.5. Quinto esempio: i divieti di uso di sistemi di IA dell'art. 5 AI Act

L'art. 5 dell'AI Act (di seguito anche "AIA")[28] vieta *inter alia* l'uso di una serie di sistemi di intelligenza artificiale ("IA").
Poiché l'uso dei sistemi di IA richiede ed include il trattamento di dati personali per finalità di addestramento, convalida, prova e *input*[29], deve ritenersi che il divieto d'uso dell'art. 5 AIA è idoneo a far ritenere senz'altro illegittima qualunque finalità di trattamento dei dati personali connessa all'uso dei sistemi di IA sottoposti al medesimo divieto, con la conseguenza che devono ritenersi invalidi in quanto illeciti i consensi *privacy* che siano prestati per queste specifiche finalità di trattamento.

5.6. Sesto esempio: lo sfruttamento delle vulnerabilità del Sig. Leon

Il successivo esempio è tratto dalle Linee guida EDPB n. 8/2020 sul *targeting* degli utenti di social media (versione 2.0 del 13 aprile 2021), dove si parla del signor Leon, il quale è fatto bersaglio di pratiche di raccolta di dati personali in grado di individuare le persone impulsive e di basso reddito, e quindi di algoritmi che su questa base decidono che persone come lui – persone (ritenute) impulsive e di basso reddito – sono il bersaglio ideale di pubblicità di scommesse *online*[30].

---

[28] Regolamento (UE) 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).
[29] Vedi le relative definizioni all'art. 3, numeri 29), 30), 32) e 33) AIA.
[30] EDPB, Linee guida 8/2020 sul targeting degli utenti dei social media. Versione 2.0, adottate il 13 aprile 2021, 27: "Esempio 8 Il signor Leon ha indicato nella propria pagina di social media di essere interessato allo sport. Ha scaricato un'applicazione sul proprio cellulare per seguire gli ultimi risultati degli incontri sportivi preferiti, ha impostato sul proprio browser la pagina www.risultatisportiviintemporeale.com come homepage sul suo portatile, usa spesso il desktop di cui dispone sul luogo di lavoro per cercare gli ultimi risultati sportivi su internet. Visita inoltre anche un certo numero di siti web di gioco d'azzardo online. Il fornitore di social media traccia l'attività online del signor Leon sui suoi molteplici dispositivi, ossia sul computer portatile, sul cellulare e sul desktop. Sulla base di tale attività e di tutte le informazioni fornite dal signor Leon, il fornitore di social media deduce che sarà interessato alle scommesse online. *Inoltre la piattaforma di social media ha sviluppato criteri di targeting*

Nelle medesime Linee guida si trova la conclusione che il Sig. Leon, fornendo un consenso *privacy* esplicito ai sensi dell'art. 22 GDPR potrebbe validamente autorizzare un trattamento dei suoi dati personali di questo tipo, permettendo così agli algoritmi di bersagliarlo in questo modo[31].

Se facciamo emergere il profilo del sindacato di liceità del consenso *privacy*, che richiede doverosamente di stabilire se le finalità di trattamento sono legittime o sono illegittime, si deve ritenere corretta la soluzione opposta a quella delineata dall'EDPB, in quanto, nell'esempio del Sig. Leon, la finalità di trattamento dei dati personali consistente – come riconosciuto dallo stesso EDPB nelle Linee guida in commento – nello *sfruttamento delle vulnerabilità* del Sig. Leon, è da ritenersi senz'altro illegittima perché in contrasto con il divieto generale delle pratiche commerciale scorrette di cui all'art. 5 UCPD (vale a dire, la direttiva 2005/29/CE sulle pratiche commerciali scorrette) e con il divieto delle pratiche commerciali aggressive in particolare[32].

---

che consentono alle imprese di rivolgersi in maniera mirata a persone che probabilmente sono impulsive e hanno un reddito più basso. La società di scommesse online «miglioriprestitiquotidiani» desidera rivolgersi agli utenti che sono interessati alle scommesse e che probabilmente scommettono somme considerevoli. Seleziona quindi i criteri offerti dal fornitore di social media per rivolgersi in maniera mirata al pubblico al quale dovrebbe essere mostrata la sua pubblicità" (https://www.edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_it_0.pdf).

[31] Le Linee guida 8/2020 in commento proseguono così argomentando a p. 28-29: "Per quanto riguarda l'esempio 8, l'EDPB ricorda che nel caso di un processo decisionale automatizzato che produce effetti giuridici che riguardano l'interessato o che incida in modo analogo significativamente sulla sua persona, come stabilito dall'articolo 22 del GDPR, i titolari del trattamento possono avvalersi delle seguenti eccezioni: • consenso esplicito dell'interessato; (…). Il Gruppo di lavoro ha già dichiarato che «*[i]n numerosi casi tipici, la decisione di proporre pubblicità mirata basata sulla profilazione non inciderà in modo analogo significativamente sulle persone [...]. Tuttavia è possibile che ciò possa accadere, a seconda delle particolari caratteristiche del caso, tra le quali: • l'invasività del processo di profilazione, compreso il tracciamento delle persone su siti web, dispositivi e servizi diversi*; *• le aspettative e le volontà delle persone interessate; • il modo in cui viene reso disponibile l'annuncio pubblicitario; oppure • lo sfruttamento della conoscenza di vulnerabilità degli interessati coinvolti*». Se la profilazione effettuata dal fornitore di social media può «[incidere] in modo analogo significativamente« su un interessato, si applica l'articolo 22. Il titolare del trattamento (o i contitolari del trattamento, a seconda del caso) dovrà (dovranno) effettuare una valutazione dell'eventualità che il *targeting* «[incida] in modo analogo significativamente» su un interessato, in ogni caso tenendo conto delle caratteristiche concrete del *targeting*. In tali circostanze, come descritto nell'esempio 8, la presentazione di pubblicità di scommesse online può rientrare nell'ambito di applicazione dell'articolo 22 GDPR (attività di *targeting* rivolta a persone finanziariamente vulnerabili interessate a scommesse online, che ha il potenziale di incidere significativamente e negativamente sulla loro situazione finanziaria). Di conseguenza, conformemente all'articolo 22, sarebbe necessario un consenso esplicito. Inoltre l'utilizzo di tecniche di tracciamento fa scattare l'applicabilità dell'articolo 5, paragrafo 3, della direttiva e-privacy, rendendo necessario il preventivo consenso da parte dell'interessato. Infine l'EDPB ricorda che il titolare del trattamento deve condurre una valutazione caso per caso rispetto alla liceità del trattamento, e che l'ottenimento del consenso non riduce gli altri obblighi relativi al rispetto delle prescrizioni in materia di correttezza, necessità, proporzionalità e qualità dei dati, di cui all'articolo 5 GDPR".

[32] V. Comunicazione della Commissione "Orientamenti sull'interpretazione e sull'applicazione della direttiva 2005/29/CE del Parlamento europeo e del Consiglio relativa alle pratiche commerciali sleali delle imprese nei confronti dei consumatori nel mercato interno" (2021/C 526/01) pubblicata sulla Gazzetta Ufficiale dell'Unione Europea del 29.12.2021, che riporta – in una serie di casistiche di pratiche da ritenersi sleali e quindi proibite ai sensi della UCPD – esempi di sfruttamento di vulnerabilità decisionale dei consumatori esattamente di questo tipo (v. il primo riquadro di esempi al par. 4.2.7, ed in particolare il primo esempio: "Un professionista riesce a capire che un adolescente è in uno stato d'animo vulnerabile a causa di eventi accaduti nella sua vita personale. Tali informazioni sono successivamente utilizzate per raggiungere l'adolescente con messaggi pubblicitari basati sulle emozioni in un momento specifico"). Sembra anche significativo osservare come il profilo funzionale sulle specifiche finalità di trattamento sia stato ritenuto rilevante dallo stesso EDPB in un parere congiunto questa volta con l'EDPS (il Garante europeo della protezione dei dati) sulla proposta di AI Act del 2021. In quel parere di appena due mesi successivo alle Linee guida in commento si legge una netta critica della previsione della proposta di AI Act di 'sdoganare', per così dire, generalmente i sistemi di intelligenza artificiale di rilevamento delle emozioni. In quel parere, al contrario si raccomanda un divieto generalizzato di sistemi di IA di questo tipo salvo

Pertanto l'eventuale consenso *privacy*, anche se esplicito *ex* art. 22 GDPR, del Sig. Leon deve ritenersi invalido in quanto illecito, perché prestato per una specifica finalità illegittima.

5.7. Settimo esempio: la piattaforma illegale di concorsi a premi

Volendo ora fare un esempio di contrasto delle specifiche finalità di trattamento con norme imperative di diritto nazionale (un secondo esempio è contenuto nel paragrafo successivo: v. par. 5.8 *infra*), possiamo fare quello di una piattaforma online che raccoglie dati personali sulla base del consenso per organizzare concorsi a premio *in violazione della normativa nazionale che regola i concorsi a premi*. Ben si danno nella realtà casi di piattaforme che non rispettano o che non rispettano integralmente la normativa di diritto pubblico che impone requisiti e limiti ai concorsi a premio[33].
A mio avviso non c'è alcun dubbio che in un simile caso anche laddove gli utenti forniscano un consenso libero, specifico, informato e non ambiguo debba ritenersi che esso sia invalido in quanto rivolto a finalità di trattamento illegittime.

5.8. Ottavo esempio: i divieti di trattamento della legge sull'oblio oncologico

Tra gli ulteriori casi di consensi *privacy* illeciti, perché prestati per trattamenti espressamente vietati dal legislatore, si può far riferimento, nel diritto italiano, alla recente legge sull'oblio oncologico, la l. n. 193/2023[34].
Al centro della l. n. 193/2023 stanno le informazioni relative allo stato di salute della persona fisica concernenti patologie oncologiche da cui la stessa sia stata precedentemente affetta e il cui trattamento attivo si sia concluso, senza episodi di recidiva, da più di dieci anni o da più di cinque anni nel caso in cui la patologia sia insorta prima del compimento del ventunesimo anno di età.
L'art. 2 l. n. 193/2023 vieta l'acquisizione e in ogni caso l'utilizzazione di tali informazioni relative ad una persona fisica contraente ai fini della determinazione delle condizioni contrattuali di qualunque tipo contratto, anche esclusivamente tra privati[35].
L'art. 3 l. n. 193/2023 introduce una serie di modifiche alla legge 4 maggio 1983, n. 184, in materia di adozione, vietando l'acquisizione e l'utilizzazione delle medesime informazioni relative alle persone che intendono adottare.

---

che per casi d'uso ben specificati, ossia si raccomanda di ammetterli solo per specifiche finalità sanitarie o di ricerca (ad esempio per pazienti per i quali il riconoscimento delle emozioni è rilevante per fini di assistenza e cura). Si legge in particolare nel Parere congiunto EDPB-GEPD 5/2021 del 18 giugno 2021, sulla proposta di Artificial Intelligence Act, al punto 35 "(…) l'EDPB e il GEPD ritengono che l'utilizzo dell'IA per dedurre le emozioni di una persona fisica sia assolutamente inopportuno e dovrebbe essere vietato, ad eccezione di taluni casi d'uso ben specificati, ossia per finalità sanitarie o di ricerca (ad esempio pazienti per i quali il riconoscimento delle emozioni è rilevante), sempre applicando idonee tutele e, naturalmente, nel rispetto di tutte le altre condizioni e restrizioni relative alla protezione dei dati, compresa la limitazione delle finalità".

[33] V. il caso di cui al già menzionato provvedimento prescrittivo e sanzionatorio del Garante per la protezione dei dati personali nei confronti di Ediscom S.A. del 23 febbraio 2023 [doc- web 9870014].

[34] Legge 7 dicembre 2023, n. 193 recante *Disposizioni per la prevenzione delle discriminazioni e la tutela dei diritti delle persone che sono state affette da malattie oncologiche*.

[35] La precisazione che il divieto riguarda anche la contrattazione tra privati esclude ogni possibilità di ricostruire il divieto come basato sulla considerazione di posizioni di debolezza contrattuale tipicamente ravvisate in situazioni di contrattazioni tra imprese e consumatori, e dunque esclude la possibilità di ricostruire la *ratio* del divieto in termini di tutela della libertà del consenso privacy.

L'art. 4 della legge 193/2023 vieta di richiedere le stesse informazioni relative a candidati ai fini dell'accesso a procedure concorsuali e selettive, pubbliche e private, anche quando nel loro ambito sia previsto l'accertamento di requisiti psico-fisici o concernenti lo stato di salute dei candidati.
Anche qui, non avrei dubbi nel ritenere invalido in quanto illecito ogni eventuale consenso *privacy* prestato dall'interessato a fronte delle condizioni che vietano il trattamento dei suoi dati personali consistenti nelle predette informazioni, ai sensi di questa disciplina.

5.9. Et cetera

Gli esempi si possono moltiplicare guardando sia ulteriori casi che non propongono difficoltà di interpretazione (consensi *privacy* relativi a trattamenti espressamente vietati dalla legge) sia a quelli che invece richiedono uno sforzo interpretativo per stabilire se una determinata finalità di trattamento di dati personali debba ritenersi illegittima, in assenza di una norma di legge che espressamente la dichiari tale o che espressamente vieti il trattamento dei dati personali. Una conclusione nel senso del divieto di trattamento di dati personali potrà ricavarsi ermeneuticamente di volta in volta in presenza di norme che (pur non vietando direttamente determinati trattamenti di dati personali) vietano determinati comportamenti o processi automatizzati i quali comportano determinati trattamenti di dati personali.
I casi sono destinati a crescere con la legislazione orientata al governo dell'industria dei dati e all'apposizione di argini giuridici alle cosiddette decisioni automatizzate e alle applicazioni digitali di tecniche che nei più varî settori utilizzano i risultati delle neuroscienze[36].
Aggiungo qui soltanto in maniera sintetica - ma spero che si capisca il contesto discorsivo dell'accenno - che anche alcuni dei più importanti tra i recenti provvedimenti del Garante *privacy* italiano, quali quelli sulla *chatbot* Replika per i bambini[37] e su ChatGPT[38] confermano

---

[36] V. A.A. MOLLO, Neurorights. *Una prospettiva di analisi interdisciplinare tra diritto e neuroscienze*, in *Annuario 2022*, cit., 191 ss.; ID., *La vulnerabilità tecnologica.* Neurorights *ed esigenze di tutela: profili etici e giuridici*, in *European Journal Of Privacy Law & Technologies*, 2021, 199 ss.; con specifico riferimento al neuromarketing, cfr. AA.VV., *Annuario 2023-2024 Osservatorio Giuridico sull'innovazione digitale*¸ a cura di S. Orlando e G. Capaldo, in corso di pubblicazione, e v. anche lo studio del marzo 2023 intitolato *State of the art of neuromarketing and its ethical implications*, commissionato e pubblicato dalla Commissione europea (https://oeuropa.eu/en/publication-detail/-/publication/43754ac8-26aa-11ee-a2d3-01aa75ed71a1/language-en).

[37] 'Replika' è una applicazione di intelligenza artificiale di tipo conversazionale che genera un personaggio virtuale programmato per instaurare conversazioni, quasi del tutto realistiche, con gli utenti e per stringere con essi legami che replicano i rapporti di amicizia o anche le relazioni sentimentali tra gli esseri umani. Secondo la presentazione dei suoi sviluppatori, tale applicazione è "capace di migliorare l'umore ed il benessere emotivo dell'utente, aiutandolo a comprendere i suoi pensieri e i suoi sentimenti, a tenere traccia del suo umore, ad apprendere capacità di *coping* - ossia, di controllo dello stress - a calmare l'ansia e a lavorare verso obiettivi come il pensiero positivo, la gestione dello stress, la socializzazione e la ricerca dell'amore". Con provvedimento n. 39 del 2 febbraio 2023, l'Autorità garante per la protezione dei dati personali ha disposto, con effetto immediato, la limitazione provvisoria del trattamento dei dati personali degli utenti stabiliti nel territorio italiano, nei confronti della società statunitense Luka Inc., sviluppatrice e gestrice della *chatbot* 'Replika', in considerazione dei concreti rischi che l'impiego di tale app presenta nei confronti dei minori di età e dei soggetti più fragili dal punto di vista emotivo (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9852506). E v. anche il successivo provvedimento sospensivo condizionato n. 280 del 22 giugno 2023 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10013893).

[38] La prima misura cautelare adottata dal Garante per la protezione dei dati personali nei confronti di OpenAI per il servizio ChatGPT con provvedimento n. 112 del 30 marzo 2023 risulta motivata, *inter alia*, come segue: "l'assenza di filtri per i minori di età di 13 anni espone gli stessi a risposte assolutamente inidonee rispetto al grado di sviluppo e autoconsapevolezza degli stessi" (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832). E v. anche il successivo provvedimento sospensivo condizionato n. 114 dell'11 aprile 2023 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702)

questa necessaria tensione verso un sindacato di legittimità sulle finalità del trattamento[39], che non è sempre agevole e che peraltro comporta, come accenneremo brevemente infra, delicate questioni di coordinamento tra diverse autorità (v. *infra* par. 7.2).

6. L'invalidità del consenso privacy per illiceità è idonea a tutelare sia l'interessato che soggetti terzi

Deve sottolinearsi che l'invalidità del consenso *privacy* per difetto del requisito di liceità è idonea a tutelare sia l'interessato (dei cui dati personali si tratti) che soggetti terzi, come nel caso dell'illiceità dei consensi *privacy* prestati per finalità di addestramento, convalida o prova dei sistemi di intelligenza artificiale sottoposti al divieto di uso ai sensi dell'art. 5 AI Act (v. *supra* par. 5.5).
Ed infatti, l'uso dei sistemi di intelligenza artificiale sottoposti al relativo divieto è considerato dal legislatore idoneo a ledere i diritti di una pluralità di persone e non solo quelli degli interessati, i cui dati personali siano processati dai sistemi di intelligenza artificiali vietati.
Gli interessati, in ipotesi, *possono non essere minacciati in alcun modo* dai sistemi di IA sottoposti al divieto di uso.
Per fare un esempio: se vengono raccolti con il loro consenso i dati personali di *persone non impulsive* per la finalità di addestrare, convalidare o provare un sistema di IA disegnato per manipolare il comportamento di *persone impulsive* sfruttando la loro vulnerabilità comportamentale derivante dall'impulsività, e che può così distorcere il loro comportamento e provocare loro un significativo danno ai sensi dell'art. 5, § 1, lett. a), AI Act, quei consensi privacy prestati dalle *persone non impulsive* dovranno senz'altro ritenersi invalidi in quanto illeciti anche se non è in gioco la lesione di loro diritti.

7. Tre aree di approfondimento.

L'ipotesi costruttiva in parola apre tre prospettive di indagine a dir poco vaste.

7.1. La finestra con vista fuori del GDPR (il test di legittimità delle finalità di trattamento non è solo endo-regolamentare)

ed il comunicato stampa del 29 gennaio 2024 sulla notifica di contestazione di violazione del GDPR (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9978020). A proposito della protezione dei minori con riferimento alla legislazione sulla protezione dei dati personali cfr. *ex multis* i contributi di I.A. CAGGIANO, *Protecting minors as technologically vulnerable persons through data protection: An analysis on the effectiveness of law.*, 2022, in *European Journal of Privacy Law & Technologies*, 27 ss.; F. RUGGERI, *Trattamento dei dati personali e tutela dei minori*, in *Annuario 2022*, cit., 325 ss. Più in generale sul tema della protezione "identitaria" dei minori nell'ambiente digitale R. SENIGAGLIA, *Rischi identitari per la persona minore di età nell'ambiente digitale*, in *European Journal of Privacy Law & Technologies*, 2023, 62 ss.; I. GARACI, *Autodeterminazione e tutela del minore di età nel contesto digitale*, in *Saggi di diritto dei consumi* a cura di A. Catricalà e M.P. Pignalosa, 2020, Torino, 115 ss.; e anche, con specifico riferimento alle tematiche del *marketing*, ID., *Profili di tutela delle persone vulnerabili nell'ecosistema digitale. Il divieto di profilazione dei minori di età ai fini di marketing*, in *Annuario 2022*, cit., 89 ss.; ID., *Minori e pubblicità mirata*, in *Dir. Merc. e Tecnologia*, 2022, 1 ss.

[39] V. anche la Relazione annuale 2023 del Presidente del Garante per la protezione dei dati personali, Prof. Pasquale Stanzione, *Regolare il futuro. La protezione dei dati per un'innovazione antropocentrica*, 8 ss.

La prima corrisponde metaforicamente ad *aprire una finestra con vista fuori del GDPR*, perché, come argomentato, il test di liceità, comportando un giudizio sulla legittimità delle finalità del trattamento e una valutazione sul se il trattamento non sia altrimenti vietato (v. parr. 3, 4, 5 *supra*), non è solo endo-regolamentare bensì deve essere condotto alla stregua di tutte le altre norme imperative del diritto dell'Unione e del diritto nazionale applicabile.
Come già visto, la necessità di guardare fuori dal GDPR è imposta innanzitutto implicitamente dal combinato disposto dell'art. 5, § 1, lett. b), GDPR con l'art. 6, § 1, lett. a), GDPR (v. parr. 3 e 4 *supra*), ma anche espressamente nell'art. 9, § 2, lett. a), GDPR a proposito del consenso esplicito (v. par. 5.1 *supra*), dove si prescrive che il consenso esplicito può superare il divieto del trattamento delle particolari categorie di dati ivi previste solo se questo non sia a sua volta vietato da altre norme del diritto dell'Unione o degli Stati membri. Dunque una finestra aperta in questo caso espressamente sulle altre norme del diritto dell'Unione o degli Stati membri. E lo stesso deve ritenersi senz'altro anche per l'altro consenso esplicito dell'art. 22, § 2, lett. a), GDPR. Ci torneremo brevemente più avanti (v. par. 7.3 *infra*). Qui è importante ribadire che è lo stesso GDPR – con il combinato disposto dei suoi artt. 5, § 1, lett. b) e 6, § 1, lett. a) e con il suo art. 9, § 1, lett. a) – ad aprire ora implicitamente ora espressamente una finestra sulle altre norme imperative del diritto unitario e nazionale applicabile per stabilire se le finalità del trattamento dei dati personali per le quali sia prestato il consenso *privacy* siano legittime e se il relativo trattamento non sia altrimenti vietato da norme inderogabili.

7.2. La questione della distribuzione di competenze tra autorità amministrative e giurisdizionali in relazione all'accertamento della legittimità/illegittimità delle finalità del trattamento

La seconda prospettiva di indagine, altrettanto ampia, riguarda *il tema di distribuzione di competenze su chi decide quali finalità di trattamento sono illegittime e quali trattamenti dei dati personali sono altrimenti vietati*. Ed infatti, se riconosciamo che il GDPR richiede di aprire una finestra sulle altre norme del diritto dell'Unione e nazionale, deve essere affrontato e risolto il tema del coordinamento tra le attività delle autorità di controllo designate per l'applicazione del GDPR nei paesi membri (le varie "DPA") e quelle delle varie autorità amministrative e giurisdizionali che hanno competenze di accertamento e sanzionatorie nei vari settori dell'ordinamento. Naturalmente c'è un livello nazionale di approfondimento e di svolgimento di questo tema, che riguarda la particolare distribuzione di competenze tra autorità nazionali, sulla base degli ordinamenti e delle norme di diritto pubblico degli Stati membri, ma c'è anche il livello del diritto dell'Unione, interpretando il quale soltanto possono essere individuate le linee generali di soluzione del problema, avuto riguardo al coordinamento tra le autorità previste dalle fonti di diritto unitario[40]. Può il Garante verificare da sé l'illegittimità delle finalità dei trattamenti dei dati personali o deve coordinarsi con altre autorità? Può o deve prendere per buone decisioni già esistenti ovvero deve chiedere decisioni di autorità giurisdizionali o di altre autorità che possono essere competenti per stabilire, come negli esempi che ho fatto prima, se un certo trattamento di dati personali è piegato a finalità illegittime o deve ritenersi altrimenti vietato sulla base di norme imperative che proibiscono determinate attività in settori presidiati da altre autorità? Si propone dunque un grande tema di coordinamento. Che si amplificherà, man mano che nuove autorità si aggiungeranno alle esistenti, come già si vede.

[40] Cfr. la sentenza CGUE del 4.7.2023 nel caso C-252/21 e le pertinenti osservazioni di P. STANZIONE, *La libertà e il suo valore*, cit., 155.

7.3. La ricerca della cassetta degli attrezzi più adeguata per affrontare le sfide ermeneutiche del consenso privacy nella data economy

Si propone, infine, un tema di svolgimento logico, che richiede innanzitutto di mettersi d'accordo su quale sia lo strumentario giuridico (la "cassetta degli attrezzi") più adeguato per trasferire sul piano dell'atto del consenso *privacy* il controllo di liceità, che è letteralmente riferito nel GDPR solo al trattamento.

La mia convinzione è che la teoria degli atti di autonomia privata fornisca lo strumentario più adeguato per compiere questo lavoro. E che, in questo senso, e per questo motivo, la teoria degli atti autonomia privata – se rettamente intesa - piuttosto che costituire una minaccia di mercificazione dei dati personali, sia, al contrario, capace di fornire una risposta di protezione.

Sembra pertinente osservare in proposito che, per attribuire validità all'atto di autonomia privata, si guarda sempre alla libertà e alla consapevolezza del suo autore, ma *anche* al profilo funzionale dell'atto, consentendo un sindacato di liceità orientato alla protezione del più ampio complesso di valori riconosciuti dall'ordinamento nella sua funzione di postulazione e affermazione deontica degli interessi dell'intera collettività[41]: ampliando così la considerazione rilevante per il giudizio di rilevanza e di tutela giuridica ben *oltre* l'ambito della protezione dei valori della libertà e della consapevolezza dell'autore dell'atto.

Deve in proposito riconoscersi che le discipline del consenso negoziale tradizionalmente contemplano requisiti di libertà e consapevolezza degli autori dell'atto di autonomia, proteggendo sempre, senza incertezze, i medesimi requisiti a cospetto di situazioni nelle quali si rinviene la necessità della loro protezione (ed articolando variamente le discipline con norme di generalità variabile intese a contrastare in ciascun caso comportamenti contrari a buona fede, anche in relazione a situazioni nelle quali il legislatore vede una minaccia di quei requisiti, come nei casi di approfittamento di situazioni di asimmetria informativa e altre situazioni di vulnerabilità decisionale)[42]; ma, anche che, *in aggiunta a ciò*, la teoria degli atti di autonomia privata prevede e impone sempre un controllo funzionale: sulla funzione dell'atto. Ed è un controllo, per così dire, ordinamentale, a protezione degli interessi della collettività.

Quindi libertà e consapevolezza dell'autore dell'atto, innanzitutto, ma al contempo anche liceità.

Esiste già d'altronde, come visto, una disposizione del GDPR che impone *espressamente* un controllo di liceità del consenso privacy. Laddove, come detto, un simile controllo deve ritenersi *implicitamente* richiesto *sempre* – alla stregua dell'art. 6(1)(a) GDPR in combinato disposto con l'art. 5(1)(b) GDPR – esso è invece *espressamente* prescritto a proposito del consenso (privacy) "esplicito" *ex* art. 9(2)(a) GDPR.

---

[41] Cfr. P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, cit., 415, dove il principio di liceità del *trattamento* è interpretato come base normativa per «selezionare i trattamenti ammessi dall'ordinamento»; e v. anche ivi, 412-413 dove osserva che il corrispondente giudizio di liceità ha per caratteristica di «contemplare una valutazione di interessi che opera su un piano (anche superindividuale e che, là dove guardi alla posizione della singola parte del rapporto (l'interessato in primo luogo), sia in grado di prescindere dalle preferenze di quest'ultimo, in ipotesi in cui queste contrastino con l'interesse della collettività». Si tratta di osservazioni pertinenti ove si osservi che la legittimità delle finalità del trattamento - rilevanti per il consenso privacy nel senso detto, per il combinato disposto delle disposizioni di cui agli artt. 5(1)(b) e 6(1)(a) GDPR – va asseverata, naturalmente, sulla base della liceità del trattamento, nel senso che non può considerarsi una finalità legittima di trattamento quella di un trattamento vietato da altre norme di legge (v. *retro*, parr. 3 e 4).

[42] Non è vero che esiste un consenso negoziale monolitico (quanto ai requisiti legali) da contrapporre a quello *privacy*, nemmeno restringendo la considerazione dell'autonomia privata all'ambito patrimoniale. Non è questa la sede per svolgere compiutamente questo tema. Ci si limita a richiamare in proposito le riflessioni esposte da ultimo proprio in relazione al dibattito del consenso privacy da G. FINOCCHIARO, *Consenso al trattamento e libertà*, cit., spec. 8 ss.; V. RICCIUTO, *Consenso al trattamento e contratto*, cit., spec. 20 ss.

Ed infatti come già osservato (v. parr. 5.1 e 7.1 *supra*) l'art. 9 del Regolamento, prevedendo al secondo paragrafo che il "consenso esplicito" possa permettere di superare il divieto del trattamento delle particolari categorie di dati elencate nel primo paragrafo, aggiunge però che un simile consenso esplicito può far superare quel divieto a meno che tale superamento ad opera di un consenso esplicito dell'interessato *non sia a sua volta vietato da altre norme di diritto dell'Unione o degli Stati Membri*.
Come anche detto, qui è inequivocabilmente disegnata una finestra che si affaccia fuori dal Regolamento (par. 7.1 *supra*).
Cosa che – aggiungo ora – a mio avviso deve ritenersi assolutamente sottintesa (tale e quale) anche nell'art. 22, § 2, GDPR.
Ed infatti – ferme restando le finalità proprie dell'art. 22 GDPR nel disegno del Regolamento e fermi restando i limiti intrinseci delle c.d. decisioni automatizzate e la loro pericolosità derivante dalle loro connaturate irrazionalità ed idoneità a realizzare discriminazioni: tratti ben messi in luce di recente dalla dottrina più avvertita[43] – a mio avviso, sul piano della tecnica del rapporto tra il primo e il secondo paragrafo dell'art. 22 del Regolamento, va riconosciuto in ogni caso che la possibilità che il consenso esplicito (del secondo paragrafo dell'art. 22 GDPR) possa far superare il divieto (del primo paragrafo dell'art. 22 GDPR) deve essere intesa e qualificata esattamente come nell'art. 9 GDPR, ossia con esclusione dei casi in cui altre norme di diritto dell'Unione o degli Stati membri non consentono al consenso esplicito di superare il divieto di assoggettarsi a decisioni che producono effetti giuridici che lo riguardano o incidono sulla sua persona basate esclusivamente sul trattamento automatizzato dei dati personali[44].
Riconoscere un limite ordinamentale al consenso privacy è tanto più urgente nello scenario attuale che ha segnato in pochi anni il trapasso dalla società dell'informazione, caratterizzata dalla riproduzione e comunicazione automatizzate di dati digitali, alla *data driven economy* o *data economy*, caratterizzata dalla *produzione automatizzata di dati digitali* (in aggiunta alla riproduzione e alla comunicazione) attraverso il trattamento di altri dati, compresi, naturalmente, dati personali. Ed effettivamente, dati che rispondono alla qualificazione giuridica di dati personali vengono continuamente non soltanto forniti dall'interessato e riprodotti con sistemi automatizzati ma anche *prodotti* da sistemi automatizzati, compresi, oggi, in parte sempre maggiore, sistemi di intelligenza artificiale[45].
Postulare, come è ovvio, che possano e debbano esserci dei limiti a questa industria dei dati, non può prescindere dall'acquisizione di strumenti della tecnica giuridica idonei a tradurre quell'idea generica di limiti in divieti giuridici e la violazione di quei divieti in precise conseguenze sul piano del trattamento degli atti di autonomia privata. In altre parole, la generica consapevolezza dell'esistenza di limiti giuridici all'industria dei dati, deve necessariamente accoppiarsi alla consapevolezza della necessità di uno strumentario giuridico da esercitarsi sul piano dell'autonomia privata.
Individuato come piano di qualificazione e costruzione del consenso *privacy* l'atto di autonomia privata, si tratterà allora di affrontare una serie di questioni tecniche con la corrispondente cassetta degli attrezzi.

---

[43] V., per tutti, D. IMBRUGLIA, *Le presunzioni delle macchine*, cit., 921 ss., spec. 930 ss. In termini più generali, A. SIMONCINI, *Do ut data: quali limiti costituzionali alla cessione di dati personali?*, in *Commerciabilità dei dati personali*, cit., 67; ID., *Il linguaggio dell'Intelligenza Artificiale e la tutela costituzionale dei diritti*, in *Rivista AIC*, n. 2, 2023. V. anche G. CARAPEZZA FIGLIA, *Decisioni algoritmiche tra diritto alla spiegazione e divieto di discriminare*, in *Pers. Merc.*, 2023, 638 ss.; A.G. GRASSO, *GDPR Feasibility and Algorithmic Non-Statutory Discrimination*, Napoli, 2023.
[44] Nello stesso senso, D. IMBRUGLIA, *Le presunzioni delle macchine*, cit., 944-945.
[45] Cfr. S. ORLANDO, *Data vs Capta. Intorno alla definizione di dati*, in *Nuovo dir. civ.*, 2022/4, 14 ss., spec. 29 ss.; GUARDA, *Il regime giuridico dei dati della ricerca scientifica*, Trento, 2021, 11 ss., 25 ss.

Si potrà così riconoscere che, a seconda del contesto nel quale si inserisce e viene prestato, l'atto di consenso *privacy* (sempre, e in ogni caso, inteso come atto di autonomia privata) può essere come può non essere qualificato come consenso contrattuale[46], ferma restando, anche nel caso in cui si tratti di un consenso contrattuale, l'applicazione dell'intero statuto del GDPR, che interviene *a conformare e limitare in modo imperativo l'autonomia privata in questo settore*[47].

Si potrà sviluppare una teoria sulla granularità causale relativamente al requisito di specificità delle finalità di trattamento dei dati personali posto dall'art. 6, § 1, lett. a), GDPR, valorizzando in proposito le norme speciali confermative di questo requisito, come quelle del DSA che prevedono che i destinatari dei servizi di piattaforme *online* possano modificare i parametri della pubblicità ad essi rivolta e le opzioni che influenzano i parametri dei sistemi di raccomandazione che determinano l'ordine delle informazioni ad essi presentate[48].

Si potrà elaborare, in coerenza con la teoria sulla granularità causale delle specifiche finalità di trattamento per le quali il consenso *privacy* è prestato, una teoria sull'invalidità parziale del consenso *privacy* relativamente a quei casi in cui alcune delle specifiche finalità di trattamento dei dati personali per cui il consenso *privacy* è prestato siano illegittime mentre altre siano legittime.

Si potrà approfondire ulteriormente il requisito della specificità della finalità posto dall'art. 6, § 1, lett. a), GDPR interrogandosi sull'idoneità di assolvere a quel requisito da parte di consensi privacy prestati in adesione a richieste che, come quasi sempre avviene, formulano le finalità in modo generico (es. finalità di *marketing*, di pubblicità, etc.), per stabilire quale debba essere la conseguenza più coerente di un difetto del requisito della specificità[49] – anche avuto riguardo all'interesse dell'interessato – sul piano del trattamento del consenso *privacy* (anche qui, come può intuirsi, sul piano del trattamento del consenso *privacy* come atto di autonomia si può giocare sul piano del consenso – quale volontà informata e consapevole – o su quello della causa e dell'oggetto), eventualmente affacciando soluzioni che, similmente a quanto può proporsi di fronte al consenso prestato per specifiche finalità legittime e per specifiche finalità illegittime, concludano, laddove se ne ravvisi un interesse dell'interessato, per una validità/invalidità parziale, ossia per la validità del consenso *privacy* per la generalità delle finalità legittime comprese nella formula generica e per una corrispondente invalidità parziale limitatamente alle finalità *illegittime* che pure possono essere ricomprese nella medesima formula generica (l'esempio della formula generica della finalità di *marketing* o pubblicità è in proposito calzante, a fronte di specifici divieti in materia: v. i numerosi esempi al par. 5 *supra*).

---

[46] È la posizione affermata con chiarezza e con nettezza da V. RICCIUTO, *Consenso e contratto*, cit. *passim*. Nello stesso senso, anche S. ORLANDO, *Il coordinamento tra la Direttiva 2019/770 e il GDPR. L'interessato-consumatore*, cit. *passim*.

[47] Parla espressamente di "*autonomia conformata* soggetta ai principi e precetti regolatori inderogabili del GDPR" E. TOSI, *Consenso autorizzatorio e consenso contrattuale quali autonome basi giuridiche per la patrimonializzazione dei dati personali nei mercati digitali alla luce del* GDPR, in *Commerciabilità dei dati personali*, cit., 229. E v. anche C. SOLINAS, *Autonomia privata e regolazione pubblica nel trattamento dei dati personali*, cit.; nonché, in una visione più generale, ID., *Il contratto "amministrato". La conformazione dell'operazione economica agli interessi generali*, Napoli, 2018; G. BERTI DE MARINIS, *Contratti dei mercati regolamentati: norme imperative e conformazione*, Napoli, 2019. V. anche S. SICA, *La monetizzazione dei dati tra autonomia privata e tutele civili*, in *Commerciabilità dei dati personali*, cit., 263.

[48] Artt. 26 e 27 DSA.

[49] Cass. 17278/2018, punto 2.6 "(…) Inoltre, ritiene il Collegio, perché il consenso possa essere detto specifico, che esso, per la contraddizione che non lo consente, non possa essere genericamente riferito a non meglio identificati messaggi pubblicitari, sicché colui il quale abbia chiesto di fruire di un servizio di informazioni giuridico-fiscali, si debba vedere poi raggiunto da pubblicità di servizi o prodotti non attinenti alle ricerche effettuate. È allora specifico, per questo aspetto, il consenso se riferito 'ad un trattamento chiaramente individuato', il che comporta la necessità, almeno, dell'indicazione dei settori merceologici o dei servizi cui i messaggi pubblicitari saranno riferiti".

Si potranno combinare insieme, in una visione funzionale, le categorie tradizionali (della tradizione dogmatica dell'atto di autonomia privata) dell'illiceità dell'oggetto e dell'illiceità della causa, in considerazione della varia articolazione dei divieti legali del contemporaneo diritto dei dati (v. parr. 4 e 5 *supra*), ed in particolare per corrispondere alla vasta tipologia dei divieti di trattamento rivolti a determinate categorie di dati personali. E così via.
Né sfuggirà che un'analisi simile può essere sviluppata *anche in relazione alla base del legittimo interesse* (art. 6, § 1, lett. f), GDPR)[50], non immune, come risaputo, dalla genericità (mi riferisco alla genericità del richiamo che ne fanno i titolari che si avvalgono di tale base, sfruttando l'ampiezza della formula legislativa), nel senso che mi sembra arrivato il momento di promuovere un sindacato di liceità *analitico* tanto sulle finalità del consenso che sul legittimo interesse, oltretutto in considerazione del fatto che oggi tanto è possibile anche dal punto di vista tecnologico, attraverso l'analisi puntuale degli algoritmi impiegati dai sistemi di intelligenza artificiale e dai sistemi software in generale[51].

8. Critica esemplare al Considerando 40 della direttiva sui lavoratori delle piattaforme online a dimostrazione della necessità di dismettere la concezione che si incentra esclusivamente sui requisiti di libertà e consapevolezza del consenso privacy

Prima di tracciare le conclusioni, mi sembra necessario aggiungere che la concezione c.d. autorizzatoria del consenso *privacy*, la quale si incentra esclusivamente sulla libertà e sulla consapevolezza dell'interessato, è ancora largamente dominante, ed al contempo indicare il limite storico di questa concezione, diventata ormai un abito mentale che ostacola il riconoscimento delle vere *rationes* di molti divieti che caratterizzano il diritto contemporaneo dei dati.
Il Considerando 40 della Direttiva sulla tutela dei lavoratori delle piattaforme *online*[52] dimostra sia il perdurante dominio di questa concezione che la sua capacità ostacolante, nel senso detto. In esso si trova infatti scritto che i molti divieti al trattamento dei dati personali dei lavoratori delle piattaforme *online*, contenuti nell'art. 7 della medesima direttiva (v. par. 5.4 *supra*), sarebbero giustificati dalla situazione di assenza di una effettiva libertà di prestare il consenso

[50] Art. 6, § 1, lett. f), GDPR: "il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore".
[51] Cfr. D. MULA, *Elaborazione e sfruttamento dei dati mediante algoritmi*, in *La circolazione dei dati*, cit., spec. 148: "Al fine di determinare se un 'trattamento svolto tramite impiego di algoritmo' è conforme alla disciplina in materia di trattamento dei dati personali, deve, quindi, ritenersi legittima l'istanza di verifica, in concreto, delle attività svolte sia in relazione alla base giuridica dichiarata che rispetto all'eventuale ambito di consenso prestato dall'interessato (…)".
[52] Considerando 40 della Direttiva relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali: "Gli articoli 5, 6 e 9 del regolamento (UE) 2016/679 stabiliscono che i dati personali devono essere trattati in modo lecito, corretto e trasparente. Ciò comporta alcune restrizioni al modo in cui le piattaforme di lavoro digitali possono trattare i dati personali mediante sistemi decisionali e di monitoraggio automatizzati. Tuttavia, nel caso specifico del lavoro mediante piattaforme digitali, non si può presumere che il consenso delle persone che svolgono un lavoro mediante piattaforme digitali al trattamento dei loro dati personali venga dato *liberamente*. Spesso le persone che svolgono un lavoro di questo tipo *non hanno una reale libertà di scelta* o non possono rifiutare o revocare il consenso senza pregiudicare il loro rapporto contrattuale, visto lo squilibrio di potere tra la persona che svolge un lavoro mediante piattaforme digitali e la piattaforma di lavoro digitale. Pertanto, le piattaforme di lavoro digitali non dovrebbero trattare i dati personali delle persone che svolgono un lavoro mediante piattaforme digitali sulla base del fatto che una persona che svolge tale lavoro ha prestato il proprio consenso al trattamento dei suoi dati personali".

privacy in cui si trovano tipicamente le persone che svolgono un lavoro mediante piattaforme digitali.
Il sottotesto di questa concezione è che, se fossero garantite effettive condizioni di libertà e consapevolezza alle persone che svolgono un lavoro mediante piattaforme digitali, o anche solo ad una categoria di tali persone, esse dovrebbero essere lasciate libere di consentire che sistemi decisionali o di monitoraggio automatizzati trattino loro dati personali relativi a loro stati emotivi o psicologici o relativi a loro conversazioni private, ivi inclusi dati riferibili al tempo in cui non lavorano, o per prevedere l'esercizio di loro diritti fondamentali (compresi il diritto di associazione, il diritto di negoziazione e il diritto di esercitare azioni collettive o il diritto all'informazione e alla consultazione), o anche per desumere la loro origine razziale o etnica, o il loro status di migrante, le loro opinioni politiche, le loro convinzioni religiose o filosofiche, loro eventuali disabilità, il loro stato di salute (comprese le malattie croniche o la sieropositività), il loro stato emotivo o psicologico, la loro adesione a sindacati, la loro vita sessuale o il loro orientamento sessuale.
La concezione autorizzatoria è dunque, evidentemente, ostacolante fino al punto da impedire perfino al legislatore europeo in sede di dichiarazione autentica della *ratio* dell'art. 7 della direttiva in commento, di sillabare la vera ragione di tutti questi divieti, e cioè che al diritto unitario ripugna un controllo automatizzato sui lavoratori di questo tipo ed una gestione automatizzata dei rapporti di lavoro di questo tipo, indipendentemente da qualunque consenso e anzi anche contro ogni eventuale consenso, libero e consapevole che sia.
Il consenso *privacy* non può essere il sinonimo di libertà di farsi perseguitare consapevolmente. Esistono dei limiti anche al consenso *privacy* libero e consapevole, che compete al legislatore fissare. La concezione del consenso *privacy* come atto di autonomia privata (o concezione negoziale) ammette questi limiti, anzi li postula come *necessari*, e consentirebbe (ovvero consentirà, quando cesserà, sperabilmente presto, il dominio della concezione che vede solo i requisiti di libertà e consapevolezza) anche allo stesso legislatore europeo di dichiararne le vere *rationes*.

9. Critica esemplare alla formula definitoria del diritto all'oblio oncologico nella legge 193/2023 a dimostrazione della necessità di evidenziare la figura logica del divieto che caratterizza il contemporaneo diritto dei dati

L'art. 1, co. 2, legge n. 193/2023 contiene la seguente definizione di "diritto all'oblio oncologico": "il diritto delle persone guarite da una patologia oncologica di non fornire informazioni né subire indagini in merito alla propria pregressa condizione patologica, nei casi di cui alla presente legge".
Tale formula definitoria non riflette le situazioni giuridiche soggettive che caratterizzano la disciplina introdotta dalla medesima legge, caratterizzata interamente, a ben vedere, dalla figura logica del divieto. La legge contiene una serie di divieti giustificati dalla previsione di minacce ad un diritto di rango costituzionale, il diritto a non essere discriminati, specificato, in casi circostanziati, come diritto delle persone fisiche a non essere discriminati a cagione della particolare condizione di una pregressa patologia oncologica. La l. n. 193/2023 contiene infatti una serie di divieti di comportamenti tipicamente ritenuti idonei a discriminare le persone fisiche a cagione di una loro pregressa patologia ontologica, e dunque a ledere questo diritto di rango costituzionale relativamente alla specifica condizione di salute considerata. Questi divieti sono formulabili come altrettanti divieti di trattamenti di determinate categorie di dati personali per determinate finalità.
La formula "diritto di non fornire informazioni" così come quella di "diritto di non essere sottoposti ad indagini" non sono soltanto inidonee a riflettere le situazioni soggettive del divieto

e del diritto costituzionale, che innervano invece la disciplina nel senso sopra esposto (e v. anche par. 5.8 *supra*). Esse sono anche fuorvianti, perché nascondono il carattere inderogabile della medesima disciplina.
In particolare, la formula "diritto di non fornire informazioni" sembrerebbe suggerire che l'interessato può comunque darle, cosicché, in quel caso, chi le riceve potrebbe tenerne conto ai fini e nei campi di applicazioni considerati dalla legge. Ciò va escluso radicalmente. Di nuovo: si tratta di divieti inderogabili di trattamento di certi dati personali per determinate finalità. E, di nuovo: l'eventuale consenso *privacy* a trattare quei dati per quelle specifiche finalità, anche laddove libero e consapevole, sarebbe illecito.
Allo stesso modo, l'espressione "diritto di non essere sottoposti ad indagini" deve tradursi come: divieto di compiere indagini.
L'esegesi delle disposizioni contenute negli articoli da 2 a 4 della l. n. 193/2023, conferma che essa contiene solo divieti inderogabili, nel senso esposto, con tutte le conseguenze che devono ricavarsene sul punto del consenso *privacy* (v. *supra* par. 5.8).
Più generalmente, e come fatto già nel paragrafo precedente a proposito del legislatore europeo, la critica a questa formula definitoria mi serve, prima delle conclusioni, per mettere in luce la perdurante difficoltà manifestata dallo stesso legislatore italiano di chiamare col suo nome la figura logica del divieto, che pure caratterizza nettamente il contemporaneo diritto dei dati e conforma l'autonomia privata in questo settore del diritto.

10. Conclusioni sul consenso privacy come atto di autonomia privata e sulla prospettiva di una nuova stagione di studi sull'atto di autonomia privata di diritto unitario sollecitata dallo studio dell'illiceità del consenso privacy.

Le osservazioni che ho provato ad esporre in questa sede possono compendiarsi in due riflessioni conclusive.
La prima è che l'autonomia privata non è da intendersi nel campo del trattamento dei dati personali come sinonimo di mercificazione dei dati personali[53], ma, tutt'al contrario, come un potenziamento della tutela della persona.
Lo studio del consenso privacy come atto di autonomia privata offre e richiede una tecnica (una 'cassetta degli attrezzi') idonea ad individuare e a tutelare non soltanto gli insopprimibili diritti fondamentali dell'interessato, ma i diritti fondamentali di tutti i consociati.
Non solo, dunque, l'insopprimibile dignità di ciascuno e di tutti gli interessati, ma – accanto ed in aggiunta ad essa – il profilo di dignità – ancora da affermare – di una collettività di persone che distinguiamo oggi dalle comunità degli uomini del passato per il fatto di vivere in un mondo caratterizzato dall'ubiquità del *software*: in cui praticamente tutti i tipi di rapporti tra gli uomini sono potenzialmente mediati da applicazioni di tecnologie digitali, che continuamente ed in modo automatizzato riproducono e producono dati.
Le norme imperative sulla protezione e la circolazione dei dati personali hanno senz'altro in questo senso un ruolo di conformazione e di limitazione dell'autonomia dei privati.
Inoltre, nella prospettiva del consenso *privacy* quale atto di autonomia regolato e dunque necessariamente limitato, dovrà riconoscersi che i limiti al consenso *privacy* possono apprezzarsi soltanto attraverso la doverosa considerazione ed applicazione di tutte le norme

[53] Assolutamente condivisibili sono le analisi sui rischi di mercificazione dei dati personali nell'attuale assetto dei mercati digitali, che si leggono in P. STANZIONE, *La libertà e il suo valore*, cit., 149 ss., spec. 152; G. CERRINA FERONI, *Siamo stati derubati? Considerazioni (non conclusive) sul valore economico dei dati personali*, in *Commerciabilità dei dati personali*, cit., 413 ss., spec. 420 ss.; A. GHIGLIA, *Commerciabilità dei dati personali: condizioni e limiti alla monetizzazione della nostra identità digitale nel contesto italiano ed europeo*, ivi, 23 ss., spec. 29.

imperative del diritto unitario e nazionale applicabile, che pongono precisi limiti all'industria dei dati. È la *finestra con vista fuori dal GDPR*, cui ho fatto cenno *supra* (par. 7.1).
Come seconda riflessione conclusiva, sembra corretto dire che le categorie del divieto e della illiceità, con le quali il giurista europeo è tenuto a cimentarsi applicando il GDPR e le altre fonti da esso chiamate in causa per stabilire la legittimità delle finalità e dell'oggetto del trattamento, offrono ai giuristi europei la possibilità di un'elaborazione nuova e storicamente adeguata sull'autonomia privata nel diritto dell'Unione: una riflessione unitaria (nel senso del diritto dell'Unione europea) sulle categorie dell'autonomia privata.
Questa prospettiva consente infatti di guardare al consenso *privacy* come ad un banco di prova per costruire intorno ad esso una *teoria dell'atto di autonomia privata di diritto europeo*.
A chi si dicesse sorpreso che la proposta di un'elaborazione di una teoria generale dell'atto di autonomia privata di diritto europeo possa originare dall'interpretazione del GDPR, risponderei che la sorpresa è fuor di luogo, per almeno tre ordini di motivi.
Innanzitutto, perché l'industria dei dati costituisce oggi il settore maggiormente in crescita nell'economia mondiale[54], e dunque non deve affatto sorprendere che a dare impulso ad una nuova stagione di studi del diritto europeo sull'autonomia privata possa essere l'analisi giuridica dei conflitti creati dalla *data economy*, a partire da quelli inerenti alla circolazione e alla protezione dei dati personali.
In secondo luogo, perché sembra corretto osservare che non siamo di fronte ad una vera opzione, in quanto le norme del GDPR *impongono* questa scelta. Ed infatti, come osservato, l'art. 5(1)(b) del Regolamento, contemplando ed *imponendo* un *test* di legittimità sulle specifiche finalità del trattamento dei dati personali, deve necessariamente accoppiarsi al profilo funzionale dell'atto di consenso *privacy*: perché, ai sensi dell'art. 6, § 1, lett. a), GDPR, l'interessato presta il consenso al trattamento "*per* una o più specifiche finalità": che *devono*, dunque, essere "legittime", né può negarsi che assumano in proposito rilevanza tutte le norme dell'ordinamento, di diritto unitario e nazionale, che, in modo via via crescente, prendono atto della esigenza di regolare l'utilizzazione e la produzione dei dati digitali, e che interpretano questa esigenza attraverso la posizione di specifici divieti di trattamento di determinate categorie di dati personali nei più vari settori.
Infine, e non meno significativamente, perché mai come oggi, con poche multinazionali – i "gate-keeper"[55] – che dispongono di risorse finanziare e tecnologiche superiori a quelle della maggior parte degli Stati[56], è improrogabile l'avvio di una nuova stagione di studî sulle funzioni degli atti di autonomia, sulla loro legittimità e sull'invalidità intesa esattamente come reazione dell'ordinamento alla violazione di specifici divieti. Uno studio storicamente avvertito sull'autonomia privata deve principiare oggi dalle categorie del divieto e della illiceità.
Sembra in proposito necessario mutarsi, perfino nel linguaggio, la concezione corrente (e che non è mai stata tecnicamente corretta) dell'autonomia privata affidata unicamente alla parola libertà (libertà negoziale, contrattuale, *freedom of contract*), disvelando, insieme alla sua dimensione di libertà, quella del dovere – due facce della stessa medaglia, l'autonomia privata

---

[54] Cfr. G. SMORTO, *Il ruolo della comparazione giuridica nella contesa per la sovranità digitale*, in *Esperienze giuridiche in dialogo*, cit. 75 ss.
[55] V. artt. 2 e 3 del *Digital Markets Act* (regolamento (UE) 2022/1925 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali))
[56] Nel comunicato stampa pubblicato sul sito web del Dipartimento di Giustizia degli Stati Uniti d'America (lo U.S. Department of Justice, Antitrust Division) a proposito di un'azione civile promossa il 21.3.2024 dal medesimo Dipartimento di Giustizia unitamente a 16 procuratori statali e distrettuali contro Apple Inc. per avere quest'ultima società pretesamente monopolizzato, o tentato di monopolizzare, i mercati connessi all'utilizzo e sviluppo degli smartphone, viene specificato che nell'anno fiscale 2023, Apple ha generato ricavi netti per 383 miliardi di dollari e un utile netto di 97 miliardi di dollari, sottolineandosi che l'utile netto di Apple supera il prodotto interno lordo di più di 100 paesi (https://www.justice.gov/opa/pr/justice-department-sues-apple-monopolizing-smartphone-markets).

essendo un potere regolato, ossia limitato dal diritto – in particolare sotto la forma del divieto: il dovere di non fare[57].
Nell'erigendo diritto europeo dei dati, il divieto è manifestato oggi in numerose norme imperative che pongono limiti precisi all'industria dei dati.
Le linee di disvelamento della faccia del divieto nella disciplina dell'autonomia privata, insieme a quella della libertà, sono ormai progressivamente sempre più evidenti nell'elaborazione della dottrina europea sugli atti di autonomia privata, anche se fin qui non si è consolidata una speculazione di questo tipo sui contratti e sugli atti di autonomia caratteristici del diritto dei dati, e sul consenso *privacy* in particolare[58].
Il governo europeo della *data economy*, offre invece, a mio avviso, un piano di applicazione ideale per costruire una teoria dell'autonomia privata di diritto europeo intorno ai divieti. Tale governo, come detto, consiste oggi nelle discipline dei numerosi atti e rapporti negoziali di condivisione dei dati previsti dalle fonti UE, che prima ricordavo (DCD, direttiva *Omnibus*, DGA, Data Act, DSA), le quali ribadiscono la prevalenza del GDPR, ma alla cui considerazione vanno aggiunti i numerosi limiti all'industria dei dati che derivano anche da tutte le altre disposizioni imperative del diritto dell'Unione e nazionale. Una loro interpretazione sistematicamente coerente è, prima che urgente, doverosa. Il piano dell'atto di autonomia privata è senz'altro idoneo ad accogliere e sviluppare, in un quadro concettuale ordinato e conosciuto, un'analisi tecnico-giuridica che possa corrispondere a questo dovere ermeneutico.

---

[57] Cfr. S. ORLANDO, *Fattispecie, comportamenti, rimedi. Per una teoria del fatto dovuto*, in *Riv. trim. dir. proc. civ.*, 2011, 1033 ss., spec. 1052 ss.

[58] Per delle osservazioni critiche sul ruolo che il sindacato sul consenso ha assunto nel diritto privato contemporaneo, v. M. FABRE-MAGNAN, *L'institution de la liberté*, PUF, Parigi, 2ª ed., 2023. Nell'ambito degli studi sull'autonomia privata, la dottrina europea ha indagato il tema dei limiti alla libertà dei privati con primario riferimento alla c.d. *freedom of contract*. Sul punto, oltre al fondamentale S. ATIYAH, *The Rise and Fall of Freedom of Contract*, Oxford University Press, Oxford, 1985, si v., almeno, M.R. MARELLA, *The Old and the New Limits to Freedom of Contract*, in *European Review of Contract Law*, 2006, 257; J. BASEDOW, *Freedom of Contract in the European Union*, in *European Review of Private Law*, 2008, 901; N. REICH, *General Principles of EU Civil Law*, Cambridge, 2013, 17; O.O. CHEREDNYCHENKO, *Freedom of Contract in the Post-Crisis Era: Quo Vadis?*, in *European Review of Contract Law*, 2014, 390; ID., *Fundamental Freedoms, Fundamental Rights, and the Many Faces of Freedom of Contract in the EU*, in *The reach of free movement*, a cura di M. Andenas, T. Bekkedal e L. Pantaleo, Asser Press, L'Aia, 2017, 273 ss.; G. VETTORI, *Diritto europeo e tutele contrattuali*, in *Pers. Merc.*, 2014, 89 ss.; S.J. WHITTAKER, *Introduction*, in *Chitty on Contracts, Volume I, General Principles*, 35ª ed., Sweet & Maxwell, Londra, 2023, ove un'interessante rassegna dei limiti che tale principio incontra nel diritto inglese, tra cui i limiti discendenti dal diritto antidiscriminatorio. Per il riconoscimento del principio del *freedom of contract* come uno dei principi generali del diritto UE, v. già l'opinione dell'A.G. Kokott nella causa CGUE C-441/07 *European Commission v Alrosa Co Ltd* (par. 225), e la sentenza della CGUE del 18.7.2013 nella causa C-426/11 Alemo-Herron e altri (par. 32). Pertinente appare anche il richiamo alle c.d. esigenze imperative (c.d. rule of reason), elaborate per la prima volta dalla CGUE nella sentenza Cassis de Dijon del 1979 (Caso 120/78), in quanto costitutive di limiti all'esercizio delle libertà fondamentali dell'Unione. Per la Commissione europea, v. già il *First Annual Progress Report on European Contract Law and the Acquis Review* COM(2005) 456 final, par. 2.6.3, nonché il Considerando 30 della proposta CESL (la proposta, poi ritirata, di Regolamento del Parlamento europeo e del Consiglio relativo a un diritto comune europeo della vendita) dove si trovava dichiarato "La libertà contrattuale dovrebbe essere il principio ispiratore del diritto comune europeo della vendita. L'autonomia delle parti andrebbe limitata solo se e in quanto indispensabile, in particolare per motivi di tutela del consumatore. Qualora ricorra simile necessità, dovrebbe essere chiaramente indicata la natura imperativa delle norme in questione". Cfr. anche l'art. 1:102 dei PECL (Principles of European Contract Law). Nel senso dell'edificazione di categorie e concetti di diritto unitario, muovendo dai problemi sottesi all'art. 82 GDPR, cfr. anche le osservazioni di C. CAMARDI, *Illecito trattamento dei dati e danno non patrimoniale. Verso una dogmatica europea*, in *Nuova giur. civ. comm.*, 2023, 1136 e U. SALANITRO, *Illecito trattamento dei dati personali e risarcimento del danno nel prisma della Corte di Giustizia*, in *Riv. dir. civ.*, 2023, 426.

DECISIONI ALGORITMICHE TRA DIRITTO ALLA SPIEGAZIONE E DIVIETO DI DISCRIMINARE

Di Gabriele Carapezza Figlia

SOMMARIO: 1. Trattamento algoritmico dei dati e rischi di discriminazione contrattuale. – 2. Divieto di decisioni totalmente automatizzate: fondamento, ambito di applicazione e limiti. – 3. Trasparenza della decisione algoritmica e diritto alla spiegazione. – 4. Inadeguatezza del paradigma dell'autodeterminazione informativa ed effettività delle tutele civili anti-discriminatorie.

1. Trattamento algoritmico dei dati e rischi di discriminazione contrattuale.

L'incidenza del paradigma anti-discriminatorio su un modello di regolamentazione del mercato che concili libertà di iniziativa economica ed eguaglianza di opportunità di accesso esige un ripensamento del tradizionale approccio al trattamento dei dati personali[1], in uno scenario nel quale l'elaborazione algoritmica è in grado di sviluppare modelli altamente predittivi, capaci di trasformare i preconcetti diffusi e radicati nell'ambiente sociale in una strategia di ottimizzazione del profitto e di allocazione efficiente delle risorse[2].
Nell'era del capitalismo digitale, l'analitica previsionale utilizza l'enorme volume di dati generati nell'infosfera[3], tanto da utenti che vivono in una dimensione collocata sul sempre più labile confine tra *online* e *offline*[4], quanto dal mondo degli oggetti interconnessi con altri dispositivi nell'*Internet of things*[5].
Il processo di elaborazione e aggregazione dei dati mediante algoritmi permette, nella *data economy*[6], una profilazione massiva allo scopo di tratteggiare, in modo sempre più sofisticato, le tendenze evolutive dei mercati, ma anche di valutare la domanda individuale di consumo a scopi di pubblicità e commercializzazione personalizzata[7]. Inoltre, lo sviluppo di sistemi di intelligenza artificiale *data driven* consente una crescente automazione degli strumenti di decisione sia in ambito pubblico sia in ambito privato, in un numero sempre più ampio di settori: dall'emanazione dei provvedimenti amministrativi all'erogazione di prestazioni sociali; dalla gestione dei processi di assunzione alla valutazione delle prestazioni dei dipendenti;

---

[1] Magistrale l'insegnamento di S. RODOTÀ, *Tecnologie e diritti*, 1ª ed., Bologna, 1995.
[2] Sviluppano una completa analisi delle nuove prospettive J. KLEINBERG, J. LUDWIG, S. MULLAINATHAN e C.R. SUNSTEIN, *Discrimination in the age of algorithms*, in *J. of Legal Analysis*, 2018, 113 ss.
[3] Una revisione teorica della nozione di dato in rapporto a quella di informazione in S. ORLANDO, *Data vs capta: intorno alla definizione di dati*, in *Nuovo dir. civ.*, 2023, 14 ss.
[4] L'acuta definizione di *onlife* per un contesto nel quale il mondo digitale *online* si mescola con quello analogico *offline* è di L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017, 27 ss.
[5] Un'aggiornata panoramica delle principali problematiche dell'*Internet of things* in G. NOTO LA DIEGA, *Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies*, Routledge, Londra, 2022.
[6] La patrimonializzazione del dato personale e la sua circolazione negoziale nella nuova economia dei dati sono approfondite lucidamente da V. RICCIUTO, *L'equivoco della privacy. Persona* v.s. *dato personale*, Napoli, 2022, sul quale v. G. CARAPEZZA FIGLIA, *"L'equivoco della* privacy". *Circolazione dei dati personali e tutela della persona*, in *Jus Civile*, 2022, 1372 ss.
[7] Osserva S. RODOTÀ, *Il diritto di avere diritti*, Roma, 2012, 329, che nella profilazione "si riflette una modellizzazione della società che produce appunto conformità più che normalità", in un effetto rafforzato dal *data mining* "poiché il modello viene individualizzato, riferito a singole persone, utilizzato in maniera mirata e selettiva".

dall'applicazione di prezzi differenziati nella vendita di beni e servizi alla stima dell'affidabilità finanziaria nella concessione di crediti[8].
Se l'impiego delle tecniche di decisione totalmente o parzialmente automatiche favorisce una razionalizzazione dei processi cognitivi, incrementando – specialmente nelle procedure caratterizzate da serialità e predeterminazione dei parametri – l'efficienza, la rapidità e l'uniformità delle scelte[9], il ricorso alla tecnologia algoritmica non è priva di elevati rischi[10].
Il trattamento automatizzato dei dati ingloba il soggetto in una *filter bubble* costruita mediante le selezioni preferenziali in rete, imprigionandolo nel suo passato[11], perché le tecniche di profilazione che elaborano i *cluster* di dati, lasciati come impronte digitali dall'utente o dai dispositivi collegati (ricerche passate; commenti; *click* precedenti; geolocalizzazioni), producono in uno schema *input-output* analisi condizionate dai dati in ingresso e dalla loro qualità[12].
Per di più, tramite l'uso di forme di intelligenza artificiale è possibile estrarre informazioni sulle caratteristiche dell'individuo non soltanto dai dati consapevolmente rilasciati, ma anche dalle c.dd. *proxies* che i sistemi di *machine learning* trasformano in predizioni spesso più accurate delle stesse informazioni fornite dagli utenti[13]. È stato dimostrato che bastano pochi *like* per identificare l'orientamento religioso di un soggetto (con una probabilità dell'82%); quello politico (con una probabilità dell'85%); il genere (con una probabilità del 93%); l'origine etnica (con una probabilità del 95%)[14]. In altri termini, il *data mining* inferisce, con enorme esattezza, attributi altrimenti invisibili, individuando relazioni statistiche da *set* di dati, che permettono di classificare gli individui in gruppi in base a criteri soltanto apparentemente neutri[15].
Molti sistemi di intelligenza artificiale sono, inoltre, delle *black box*, delle quali conosciamo gli *input* e gli *output* ma non i meccanismi di funzionamento, che rischiano di razionalizzare pregiudizi socialmente diffusi o di generare discriminazioni inconsapevoli[16].

---

[8] V., utilmente, M. DELMASTRO e A. NICITA, *Big data. Come stanno cambiando il nostro mondo*, Bologna, 2019, 14 ss.
[9] In questo senso, G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Pol. dir.*, 2019, 211 ss., il quale osserva che "l'automazione del processo decisionale» risulta «astrattamente in linea, non soltanto con le istanze di calcolabilità delle relazioni di mercato, ma anche con i canoni di efficienza ed economicità dell'azione amministrativa".
[10] Una lucida identificazione dei rischi sottesi all'elaborazione algoritmica in P. PERLINGIERI, *Relazione conclusiva*, in ID., S. GIOVA e I. PRISCO (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, Napoli, 2020, 379 ss., il quale rileva l'esigenza di controllare "i risultati prodotti verificandone la compatibilità con il sistema ordinamentale" (p. 380 s.). In argomento cfr., altresì, C. PERLINGIERI, *Diritto privato delle nuove tecnologie: contenuti e competenze*, in *Tecnologie e diritto*, 2021, 70 ss.; E. BATTELLI, *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e diritti della persona*, in *Dir. fam. pers.*, 2022, 1096 ss.
[11] Si rinvia a E. PARISER, *The Filter Bubble: What The Internet Is Hiding From You*, Penguin Press, New York, 2011, sul quale v. M. BIANCA, *La filter bubble e il problema dell'identità digitale*, in *Medialaws*, 2019, 39 ss.
[12] Evidenzia D. IMBRUGLIA, *Le presunzioni delle macchine e il consenso dell'interessato*, in *Riv. trim. dir. proc. civ.*, 2023, 927, che nelle tecniche di *machine learning* la "modalità di elaborazione dell'algoritmo differisce da quella dei *software* c.dd. tradizionali", perché "la formazione dell'inferenza è interamente automatizzata", sì che lo sviluppo della presunzione è svolto interamente dalla macchina.
[13] Un approfondimento sull'attitudine delle tecniche predittive a incorporare *biases* presenti nella selezione dei dati rilevanti in D. KEATS CITRON e F. PASQUALE, *The Scored Society: Due Process for Automated Predictions*, in *Washington L. Rev.*, 89, 1, 2014, 1 ss.
[14] Si tratta dello studio di M. KOSINSKI, D. STILLWELL e T. GRAEPEL, *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, in *Proceedings of the National Academy of Sciences*, 2013, 5802 ss.
[15] Cfr. M. DELMASTRO e A. NICITA, *op. cit.*, 35 s.
[16] "Human decisions are frequently opaque to outsiders, and they may not be much more transparent to insiders": J. KLEINBERG, J. LUDWIG, S. MULLAINATHAN e C.R. SUNSTEIN, *op. cit.*, 113. V., più ampiamente, F. PASQUALE, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge, 2015.

Nei sistemi di *machine learning* possono svilupparsi *statistical biases*[17], perché ora i decisori camuffano discriminazioni intenzionali con la programmazione dell'algoritmo, ora i dati utilizzati come *input* riflettono indirettamente un pregiudizio, ricorrendo con maggiore frequenza nei gruppi sociali 'svantaggiati'[18], ora i *set* di dati non sono sufficientemente rappresentativi, in quanto le classi di individui portatrici di un fattore di rischio risultano sottodimensionate rispetto alla popolazione generale[19].
Rimangono celebri alcuni casi: il *software* COMPAS adoperato negli Stati Uniti per la predizione del rischio di recidive di soggetti sottoposti a procedimenti penali, che è stato giudicato conforme al *due process of law*, nonostante evidenziasse un pregiudizio sistematico nei confronti degli afroamericani[20]; l'algoritmo impiegato nel Regno Unito e in Irlanda per la valutazione conclusiva dei risultati di apprendimento degli studenti, che discriminava quelli ad alto rendimento in relazione alla localizzazione degli istituti scolastici[21]; il sistema di riconoscimento facciale automatico utilizzato dalla polizia gallese, che è stato considerato non scevro dall'influenza di fattori quali il genere e l'origine etnica dei soggetti controllati[22].
Nelle tecniche di *big data analytics*, allora, il processo prognostico sembra cristallizzare un "determinato «stato del mondo»"[23], incorporando i preconcetti sociali nei dati di apprendimento capaci di guidare le funzioni predittive, così da influenzare i risultati ottenuti e i conseguenti processi decisionali. Negli scambi *online*, anzi, il trattamento algoritmico dei dati – con le sue spiccate capacità di aggregare gli individui per una loro caratteristica rilevante – può perpetuare e amplificare i pregiudizi diffusi[24], in misura enormemente maggiore rispetto ai mercati *offline*[25], impedendo automaticamente ai membri del gruppo svantaggiato l'accesso al bene o servizio scambiato o imponendo loro condizioni contrattuali diverse o peggiori[26].
La costruzione algoritmica delle classi, in base a una selezione delle caratteristiche rilevanti degli individui, incide allora sulla *equal opportunity* di accesso al mercato, generando risultati che mascherano, sotto le vesti di una valutazione di ordine logico, giudizi di valore, dei quali

---

[17] Illustra accuratamente i diversi fattori che possono celarsi alla radice dell'effetto discriminatorio dell'algoritmo, G. RESTA, *op. cit.*, 217 s.
[18] "While these correlations may be «true» in the sense of statistical validity, we societally and politically often wish they weren't": L. EDWARDS e M. VEALE, *Slave to the Algorithm? Why a "Right to an Explanation" Is Probably not the Remedy You Are Looking for*, in *Duke L. Tech. Rev.*, 2017, 16 e 28 s.
[19] La sottorappresentazione di alcuni strati della popolazione nei *big data* utilizzati dalle intelligenze artificiali è rilevata da J. LERMAN, *Big data and Its Exclusions*, in *Stan. L. Rev. Online*, 2013, 55, il quale propone di sviluppare "a new legal doctrine" – definita "data antisubordination" – "to protect those persons whom the big data revolution risks sidelining".
[20] Si tratta della decisione resa dalla Supreme Court del Wisconsin nel caso *State v. Loomis*, 881 N.W.2d 749, 2016, ove la violazione del *due process* è esclusa poiché il dispositivo COMPAS costituiva soltanto uno dei fattori impiegati per la determinazione della misura sanzionatoria.
[21] Per una dettagliata analisi, v. E. FALLETTI, *Discriminazione algoritmica. Una prospettiva comparata*, Torino, 2022, 250 ss.
[22] La decisione della *Court of Appeal* nel caso *R. (on the application of Bridges)* v. *Chief Constable of South Wales Police*, [2020] EWCA Civ 1058 è commentata da G. GIORGINI PIGNATIELLO, *Il contrasto alle discriminazioni algoritmiche: dall'anarchia giuridica alle Digital Authorities?*, in *Federalismi.it*, 2021, 179.
[23] In questi termini, G. RESTA, *op. cit.*, 214, il quale rileva che le tecniche di *big data analytics* hanno "la propensione a «codificare» il passato, ingabbiando soluzioni e predizioni all'interno delle griglie fornite dai trascorsi storici e dal set di valori che ha guidato la programmazione del sistema".
[24] Sul rischio che, con l'impiego massiccio di tecniche decisionali algoritmiche, "societies are destined to continue to reinforce patterns of entrenched privilege and disadvantage, widening gaps between rich and poor, and perpetuation of disadvantage", v. J. WOLFF e A. DE-SHALIT, *Disadvantage*, Oxford University Press, Oxford, 2007, 186.
[25] Le ragioni della persistenza delle discriminazioni nei mercati sono evidenziate da C.R. SUNSTEIN, *Why Markets Won't Stop Discrimination*, in *Soc. Phil. Pol.*, 1991, 8 e 22 ss.
[26] Sul concetto normativo di discriminazione sia consentito rinviare a G. CARAPEZZA FIGLIA, *Divieto di discriminazione e autonomia contrattuale*, Napoli, 2013, 73 ss.

occorre verificare la compatibilità con i princípi fondamentali del sistema ordinamentale[27]. A questa sfida l'interprete può rispondere oggi non soltanto attingendo allo strumentario offerto dalla disciplina in materia di tutela dei dati personali, ma anche avvalendosi della normativa antidiscriminatoria, che impone di giustificare l'effetto di diseguaglianza creato dai poteri in senso lato normativi nei rapporti intersoggettivi di diritto privato[28].

2. Divieto di decisioni totalmente automatizzate: fondamento, ambito di applicazione e limiti.

La tutela della persona contro la discriminazione algoritmica rinviene un primo momento di emersione nel tessuto normativo del GDPR[29], il quale affronta tanto la questione delle condizioni di liceità quanto quella della trasparenza dei procedimenti di profilazione e decisione automatica[30].
In particolare, tenuto conto di quanto previsto dal Considerando 71, l'art. 22 GDPR riconosce a ogni individuo il "diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona" (art. 22, § 1, GDPR)[31].
Si tratta di "una norma generale sulla distribuzione del potere di decisione nel mondo digitale"[32], ispirata al rispetto del principio di dignità[33], che prevede un vero e proprio divieto oggettivo di decisioni rilevanti sul piano personale fondate sulle previsioni macchiniche, offrendo una tutela di ampia portata dagli effetti pregiudizievoli del trattamento automatizzato, senza richiedere l'esercizio di un diritto di opposizione da parte dell'interessato[34].
Il divieto si applica ai processi decisionali totalmente basati sul trattamento automatizzato, privi cioè di un coinvolgimento umano rilevante. In altri termini, non sono proibite le decisioni adottate a valle di un trattamento automatico, purché intervenga nella valutazione un contributo umano che non sia minimo o meramente simbolico, ma comporti un riesame del processo in

[27] Rileva P. FEMIA, *Interessi e conflitti culturali nell'autonomia privata e nella responsabilità civile*, Napoli, 1996, 540, nota 843, che "la decisione di aggregare individui per una loro caratteristica rilevante deve essere controllata, come giudizio di valore, nella sua congruenza con l'intreccio dei valori costituzionali richiamati nella fattispecie". Più di recente cfr. ID., *Discriminazione (divieto di)*, in *Enc. dir.*, *I tematici*, I, Milano, 2021, 499 ss.
[28] Si veda, volendo, G. CARAPEZZA FIGLIA, *Il divieto di discriminazione quale limite all'autonomia contrattuale*, in *Riv. dir. civ.*, 2015, 1405 ss.
[29] Una riflessione sul coagularsi della disciplina del GDPR intorno al valore della persona umana in V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Contr. impr.*, 2018, 1098 ss.
[30] Cfr., in argomento, E. PALMERINI, *Algoritmi e decisioni automatizzate. Tutele esistenti e linee evolutive della regolazione*, in *I diritti fondamentali nell'era della digital mass surveillance*, a cura di L. Efrén Ríos Vega, L. Scaffardi e I. Spigno, Napoli, 2019, 209 ss.
[31] V., per un articolato approfondimento della disciplina racchiusa nell'art. 22 GDPR, A.G. GRASSO, *GDPR Feasibility and Algorithmic Non-Statutory Discrimination*, Napoli, 2023, 29 ss., secondo il quale essa "is far from being an easily interpretable provision". Le 'tre condizioni cumulative' di applicabilità della disposizione sono analizzate accuratamente da Corte giust., 7 dicembre 2023, c. 634/21, OQ c. Land Hessen, § 43 ss.
[32] Così, S. RODOTÀ, *Il diritto di avere diritti*, cit., 328.
[33] In questi termini, G. RESTA, *op. cit.*, 222, secondo il quale la proibizione evita "che la persona sia resa oggetto passivo di decisioni assunte in forma deumanizzata".
[34] Cfr. Gruppo di lavoro art. 29 per la protezione dei dati, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 25, ove si aggiunge che "effetti significativi possono risultare anche da azioni di persone diverse dalla persona alla quale fa riferimento la decisione automatizzata".

grado di esercitare un'influenza sul risultato finale[35]. Una differenza che suscita perplessità, in virtù della diffusa tendenza alla ricezione integrale delle decisioni delle intelligenze artificiali, che gli agenti umani propendono a qualificare come razionali[36].
Occorre, inoltre, che gli effetti della decisione sulla sfera dell'interessato siano significativi[37]. Il Considerando 71 offre due esempi "quali il rifiuto automatico di una domanda di credito *online* o pratiche di assunzione elettronica senza interventi umani", che le Linee guida elaborate dal Comitato europeo per la protezione dei dati arricchiscono ulteriormente, precisando che vanno, comunque, considerati rilevanti – oltre agli effetti "in grado di incidere in maniera significativa sulle circostanze, sul comportamento o sulle scelte dell'interessato" e quelli che hanno "un impatto prolungato o permanente sull'interessato" – gli effetti discriminatori, compreso il *dynamic pricing*, ogni qual volta "prezzi proibitivi elevati impediscono effettivamente a una persona di ottenere determinati beni o servizi"[38].
Nell'ambito applicativo del divieto è incerto se rientri anche il *marketing online* basato sulla profilazione. Una soluzione affermativa appare preferibile quando le conseguenze prodotte dal *microtargeting* sulla sfera individuale raggiungano una soglia rilevante, come accade nelle ipotesi di c.d. *weblining* ove sia potenzialmente escluso o ristretto l'accesso a beni o servizi da parte dei membri di determinati gruppi sociali (ad esempio, qualora i sistemi di ricerca *online* di abitazioni orientino gli utenti verso differenti zone in base all'origine etnica) oppure in quelle – che potrebbero altresì incorrere nel divieto di pratiche commerciali aggressive *ex* art. 25, 1° co., lett. d, Codice del Consumo – ove sia limitata la libertà di scelta o di comportamento di consumatori vulnerabili (ad esempio, qualora annunci pubblicitari di prodotti finanziari ad alto rischio siano rivolti in modo invasivo a destinatari dei quali si conoscano le effettive o probabili difficoltà economiche)[39].
Il divieto di decisioni automatizzate conosce significative eccezioni, in presenza di specifici presupposti di liceità, quali la necessità per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; l'autorizzazione da parte di una previsione di legge; il consenso esplicito dell'interessato (art. 22, § 2, GDPR)[40].
Tuttavia, alle ipotesi di decisioni automatizzate fondate sulle basi giuridiche della necessità per la conclusione o l'esecuzione di un contratto e del consenso esplicito, sono correlate incisive forme di tutela[41], giacché il titolare è tenuto ad adottare misure appropriate per salvaguardare

---

[35] Si rinvia alle attente considerazioni di E. PELLECCHIA, *Profilazione e decisioni automatizzate al tempo della* black box society*: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, in *Nuove leggi civ. comm.*, 2018, 1223 ss.
[36] Sottolinea R. CATERINA, *Autonomia e intelligenza artificiale*, in *Il trattamento algoritmico*, cit., 142, che "l'essere umano non ha in concreto gli strumenti per sottoporre a vaglio critico i risultati elaborati dall'intelligenza artificiale, e dunque non può che recepirli integralmente".
[37] Discorre di "ampia portata rivestita dalla nozione di «decisione»", Corte giust., 7 dicembre 2023, c. 634/21, OQ c. Land Hessen, §§ 44-45, secondo la quale essa "rinvia non solo ad atti che producono effetti giuridici riguardanti il soggetto di cui trattasi, ma anche ad atti che incidono significativamente su di esso in modo analogo".
[38] Cfr. Gruppo di lavoro art. 29 per la protezione dei dati, *op. cit.*, 21. Osserva acutamente A. FEDERICO, *Equilibrio e contrattazione algoritmica*, in *Rass. dir. civ.*, 2021, 515 s., che "le nuove tecnologie consentono agli operatori commerciali di individuare la specifica disponibilità di pagamento di ogni cliente senza ricorrere a negoziazioni individuali". Sul *dynamic pricing* v., altresì, F.Z. BORGESIUS, *Price discrimination, algorithmic decision-making, and European non-discrimination law*, in *European Business L. Rev.*, 2019, 401 ss.
[39] Comunicazione della Commissione *Una strategia europea per i dati* COM/2020/66 *final* del 19 febbraio 2020, disponibile su *eur-lex.europa.eu*.
[40] Secondo R. MESSINETTI, *La tutela della persona umana* versus *l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contr. impr.*, 2019, 890, "la vulnerabilità della persona esposta al potere decisionale dell'apparato tecnologico è la chiave per comprendere il senso del divieto generale posto dall'art. 22 GDPR e perciò della dialettica regola-eccezione che questa norma definisce".
[41] Osserva A.G. GRASSO, *op. cit.*, 74 s.: "Their effectiveness depends first and foremost on the quality, quantity and, above all, relevance of the information and explanations that the data subject can receive from the controller".

l'interessato, garantendo "almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione" (art. 22, § 3, GDPR)[42]. In altri termini, anche quando è lecito che il processo decisionale sia basato unicamente su un trattamento automatizzato, l'interessato conserva il diritto a qualche forma di partecipazione umana (c.d. *human in the loop*) che controlli, confermi o smentisca il risultato finale[43].

Allo scopo di sottrarre al trattamento algoritmico il nucleo di dati che meritano maggiore protezione per la loro inerenza all'identità della persona e ai suoi diritti fondamentali, le decisioni automatizzate permesse non possono avvalersi, in ogni caso, delle categorie particolari di dati personali previste dall'art. 9, § 1, GDPR[44], salvo che l'interessato abbia prestato il proprio consenso esplicito o il trattamento sia necessario per motivi di interesse pubblico, dovendo comunque applicarsi misure adeguate di protezione degli interessi coinvolti (art. 22, § 4, GDPR).

Oltre a definire l'area di liceità delle decisioni prese come risultato dell'elaborazione automatizzata dei dati[45], il Regolamento persegue la finalità di escludere che il procedimento di profilazione e decisione automatica possa avvenire in modo occulto, in attuazione del principio di trasparenza che conforma intensamente le situazioni soggettive del titolare e dell'interessato[46].

In tal senso, sono previsti specifici obblighi di informazione che si articolano diversamente nelle due fasi, distinte non soltanto cronologicamente, della raccolta dei dati e dell'esecuzione del trattamento[47].

Innanzitutto, allo scopo di garantire un trattamento corretto e trasparente, l'informativa, prevista al momento della raccolta dei dati presso l'interessato o un soggetto diverso, deve riferirsi in modo specifico e intellegibile all'esistenza di un processo decisionale automatizzato, compresa la profilazione e fornire, almeno nei casi di decisione totalmente automatica, "informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato" (artt. 13, § 2, lett. f) e 14, § 2, lett. g), GDPR)[48].

In secondo luogo, il medesimo interesse conoscitivo è soddisfatto mediante l'esercizio, da parte dell'interessato, del diritto di accesso, anche quando il trattamento sia iniziato, sia in corso di esecuzione o abbia già prodotto una decisione (art. 15, § 1, lett. h), GDPR)[49].

---

[42] Sostiene che i diritti sono organizzati in una logica ascendente dalla richiesta di intervento umano sino al controllo giurisdizionale, C. SARRA, *Put Dialectics into the Machine: Protection against Automatic-decision-making through a Deeper Understanding of Contestability by Design*, in *Global Jurist*, 2020, XX, 3, 8.

[43] Discorre di "principio di non esclusività della decisione algoritmica", Cons. St., 4 febbraio 2020, n. 881, il quale esclude che possa postularsi "una coincidenza fra la legalità e le operazioni algoritmiche", occorrendo invece che siano sempre provate sul piano tecnico "le istruzioni impartite e le modalità di funzionamento delle operazioni informatiche se ed in quanto ricostruibili sul piano effettuale perché dipendenti dalla preventiva, eventualmente contemporanea o successiva azione umana di impostazione e/o controllo dello strumento".

[44] Un approfondimento sulle categorie particolari di dati in A. THIENE, *sub art. 9*, in *Codice della privacy e data protection*, a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta, Milano, 240 ss.

[45] Si rinvia a M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio e V. Ricciuto, Torino, 2019, 179 ss.

[46] In tema, v. l'approfondita indagine di J.A. KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON e H. YU, *Accountable Algorithms*, in *University Pennsylvania L. Rev.*, 2017, 165, 633 s., secondo i quali "the central issue is how to assure the interests of citizens, and society as a whole, in making these processes more accountable".

[47] Un inquadramento generale degli obblighi di informazione in R. ALESSI, *Gli obblighi di informazione tra regole di protezione del consumatore e diritto contrattuale europeo uniforme e opzionale*, in *Eur. dir. priv.*, 2013, 311 ss.

[48] Un'interpretazione sistematica degli artt. 13 e 14 GDPR tale da valorizzare la leggibilità dell'algoritmo nelle ipotesi di decisioni automatizzate è proposta da G. COMANDÉ, *Leggibilità algoritmica e consenso al trattamento dei dati personali. Note a margine di recenti provvedimenti sui dati personali*, in *Danno e resp.*, 2022, 141 ss.

[49] Cfr. A. SPANGARO, *Il concetto di profilazione tra "direttiva madre" e GDPR*, in *Giur. it.*, 2022, 1557 ss.

Nei rapporti di consumo, infine, il principio di trasparenza rinviene una specifica declinazione nella previsione racchiusa nell'art. 49, 1° co., lett. e-*bis*), Codice del Consumo (introdotto dal D.Lg. 7 marzo 2023, n. 26, in attuazione dell'art. 4 Direttiva (UE) 2019/2161), che impone al professionista di fornire al consumatore "l'informazione che il prezzo è stato personalizzato sulla base di un processo decisionale automatizzato"[50], prima che sia vincolato da un contratto a distanza o negoziato fuori dei locali commerciali o da una corrispondente offerta[51].

3. Trasparenza della decisione algoritmica e diritto alla spiegazione.

L'interpretazione sistematica del riferito quadro normativo, anche alla luce del Considerando 71 GDPR[52], permette di configurare un diritto alla trasparenza della decisione algoritmica, che assume un contenuto rafforzato in ragione del carattere totalmente automatico del procedimento. Se, infatti, all'interessato, è attribuito, in ogni caso, il diritto a essere informato che il trattamento dei suoi dati azioni un processo decisionale automatizzato, la posizione soggettiva si arricchisce quando è escluso ogni intervento umano significativo, trasformandosi in un vero e proprio diritto alla spiegazione della decisione[53], che impone la leggibilità dell'algoritmo con riferimento alle sue possibili conseguenze sulla sfera giuridica dell'interessato.
La trasparenza, in grado di prevalere nel bilanciamento con i diritti di proprietà intellettuale e di proprietà industriale relativi al *software*[54] non richiede di svelare in modo completo l'algoritmo o le sue modalità tecniche di funzionamento, esigendo piuttosto un'informazione adeguata a rendere comprensibili i motivi alla base della decisione dell'agente intelligente[55].
Se, dunque, nell'esercizio dell'attività amministrativa vincolata o discrezionale, secondo il Consiglio di Stato, il principio di trasparenza subordina l'utilizzo degli algoritmi, "in sede decisoria pubblica", alla "piena conoscibilità a monte del modulo utilizzato e dei criteri applicati", allo scopo di assicurare che "i criteri, i presupposti e gli esiti del procedimento robotizzato siano conformi alle prescrizioni e alle finalità stabilite dalla legge o dalla stessa amministrazione"[56]; nel campo delle decisioni prese da soggetti privati va assicurata, piuttosto,

---

[50] Sul punto v. A. FEDERICO, *Equilibrio e contrattazione algoritmica*, cit., 516 s.
[51] Una riflessione sui rapporti tra tutela dei dati personali e disciplina consumeristica in S. PAGLIANTINI, *L'interferenza ascosa tra GDPR e diritto dei consumatori: appunti per una tassonomia*, in *Giur. it.*, 2023, 2212 ss.
[52] Avverte del rischio insito in un'interpretazione meramente esegetica delle singole disposizioni in materia di tutela dei dati personali, P. PERLINGIERI, *Sul trattamento algoritmico dei dati*, in *Tecnologie e diritto*, 2020, 184.
[53] In diversa prospettiva, S. WACHTER, B. MITTELSTADT e L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation,* in *Int. Data Privacy L.*, 2017, 76 ss., che argomentano in base all'intenzione del legislatore europeo di escludere un diritto alla spiegazione *ex post* di specifiche decisioni automatiche.
[54] Il Considerando 63 GDPR stabilisce che il diritto di accesso ai dati personali da parte dell'interessato "non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software". Tuttavia, secondo G. RESTA, *op. cit.*, 224 s., è auspicabile "optare per un'interpretazione restrittiva della clausola di salvaguardia (…), in linea peraltro con quanto espresso nei Considerando 34 e 35 della direttiva 2016/943/UE sulla protezione dei segreti commerciali". In argomento v., altresì, G. MALGIERI, *Trade Secrets v. Personal Data: a Possible Solution for Balancing Rights*, in *Int. Data Privacy L.*, 2016, 102 ss.
[55] V., *amplius*, G. MALGIERI e G. COMANDÉ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data-Protection Regulation*, in *Int. Data Privacy L.*, 2017, 7, 243 ss.
[56] V., nella giurisprudenza amministrativa, Cons. St., 4 febbraio 2020, n. 881, cit.; Cons. St., 8 aprile 2019, n. 2270, secondo il quale "la regola algoritmica deve essere non solo conoscibile in sé, ma anche soggetta alla piena cognizione, e al pieno sindacato, del giudice amministrativo"; nonché T.A.R. Lazio, 21 marzo 2017, n. 3742 e T.A.R. Lazio, 22 marzo 2017, n. 3769, in *Dir. inf.*, 2019, 979 ss., con commento di E. PROSPERETTI, *Accesso al* software *e al relativo algoritmo nei procedimenti amministrativi e giudiziali. Un'analisi a partire da due pronunce*

la leggibilità della "formula tecnica", rendendo chiara la modalità della sua traduzione in regola giuridica del caso concreto[57].
Pertanto, l'utilizzazione dello strumento algoritmico fa sorgere in capo al soggetto che tratti i dati in maniera automatizzata un obbligo di informazione di intensità crescente che abbraccia, nel caso di integrale sostituzione della macchina all'intervento umano, non semplicemente la logica generale di funzionamento del *software*, ma l'*iter* procedimentale che conduce all'assunzione della decisione nei confronti di un singolo individuo. Si tratta, con le parole del Garante europeo della protezione dei dati, di una "*disclosure of the «logic of decision-making»*" che richiede di divulgare, ad esempio, i parametri sui quali si fonda la personalizzazione delle condizioni dei contratti di assicurazione sulla circolazione dei veicoli[58]; il *credit scoring* nelle procedure di finanziamento[59]; la strutturazione variabile dei prezzi di beni e servizi nei rapporti *online*[60].
Le elaborazioni giurisprudenziali, tra l'altro, sembrano conferire al diritto alla leggibilità dell'algoritmo una tendenza espansiva, individuando l'informazione sulla logica decisionale quale requisito indispensabile per la formazione di un consenso libero e consapevole, anche per la sua attitudine a condizionare l'esercizio del potere di controllo dell'interessato sulla circolazione dei propri dati[61]. In particolare, una recente decisione della Suprema Corte, resa in materia di elaborazione macchinica dei profili reputazionali, ha messo in luce l'essenzialità della trasparenza dell'algoritmo di calcolo del *rating* per la formazione di una valida determinazione di volontà, sì da escludere la liceità del trattamento automatizzato se manchi la consapevolezza da parte dell'interessato dello schema esecutivo dell'algoritmo e degli elementi che lo compongono[62]. La spiegazione *ex ante* del funzionamento del meccanismo decisionale,

---

del Tar Lazio. Una sensibile riflessione sul tema in G. DI ROSA, *Quali regole per i sistemi automatizzati "intelligenti"?*, in *Riv. dir. civ.*, 2021, 828 ss.

[57] Si rinvia ad A.G. GRASSO, *op. cit.*, 74 ss., per un'attenta ricostruzione del dibattito "whether the data subject is only entitled to a general ex ante explanation of how the algorithm works, or a right to an ex post explanation of the decision concretely and individually made against him or her".

[58] È noto che – secondo Corte giust., Grande Sez., 1 marzo 2011, c. 236/09, Association Belge des Consommateurs Test-Achats e a. c. Conseil de Ministres – deve considerarsi contrario al principio della parità di trattamento tra donne e uomini (artt. 21 e 23 Carta dir. fond. Un. eur. e dir. 2004/113) mantenere, senza limiti di tempo, una deroga alla regola dei premi e delle prestazioni *unisex* nel settore dei servizi assicurativi.

[59] Secondo Corte giust., 7 dicembre 2023, c. 634/21, OQ c. Land Hessen, il calcolo automatizzato di un tasso di probabilità basato su dati personali relativi alla capacità di onorare gli impegni di pagamento costituisce un "processo decisionale automatizzato" ai sensi dell'art. 22 GDPR, "qualora da tale tasso di probabilità dipenda in modo decisivo la stipula, l'esecuzione o la cessazione di un rapporto contrattuale con tale persona da parte di un terzo al quale è comunicato tale tasso di probabilità". Sul problema della trasparenza degli algoritmi nel sistema di *credit scoring*, v. P. MANES, *Credit scoring assicurativo, machine learning e profilo di rischio: nuove prospettive*, in *Contr. impr.*, 2021, 469 ss.

[60] Cfr. EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 7/2015. Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability*, 19 novembre 2015, 16, 19, dove si specifica: "Some everyday examples where «the logic of decision-making» should be disclosed include a personalised car insurance scheme (using car sensor data to judge driving habits); credit scoring services; a pricing and marketing system that determines how much discount an individual will receive, or what media content to recommend to an individual".

[61] Osserva R. MESSINETTI, *La tutela della persona umana versus l'intelligenza artificiale*, 890, che il diritto di ottenere una spiegazione significativa della logica sottostante al processo decisionale automatizzato "costituisce il *medium* necessario per l'esercizio di poteri fondamentali nei confronti dell'I.A.: *in primis* quello di contestarne la decision"».

[62] Cfr. Cass., ord., 25 maggio 2021, n. 14381, in *Rass. dir. civ.*, 2022, 367 ss., con nota di M. TANZILLO, *Rating reputazionale tra consenso dell'interessato e princípi dell'ordinamento italo-europeo*, secondo la quale, in relazione ad algoritmi reputazionali, "non può logicamente affermarsi che l'adesione alla piattaforma da parte dei consociati comprenda anche l'accettazione di un sistema automatizzato, che si avvale di un algoritmo, per la valutazione oggettiva di dati personali, laddove non siano resi conoscibili lo schema esecutivo in cui l'algoritmo si esprime e gli elementi all'uopo considerati".

integrata tra i presupposti necessari per la libertà del consenso, è iscritta così nella cornice generale all'interno della quale il trattamento dei dati può considerarsi lecito, concretizzando la correttezza del comportamento del titolare e concorrendo ad assicurare la specificità del consenso dell'interessato.

4. Inadeguatezza del paradigma dell'autodeterminazione informativa ed effettività delle tutele civili anti-discriminatorie.

L'impostazione del GDPR affronta il problema del rischio della decisione algoritmica, enfatizzando maggiormente il versante dell'intelligibilità della logica sottostante al processo decisionale, rispetto a quello dei potenziali effetti discriminatori[63].
La *digital regulation* del Regolamento si ispira, infatti, al paradigma dell'autodeterminazione informativa, riconducendo il fenomeno delle decisioni matematicamente formalizzate ai principi generali che ispirano il regime della circolazione dei dati personali, con l'obiettivo tanto di assoggettare le attività di trattamento a una stringente valutazione di liceità, quanto di assicurare all'interessato un *set* di diritti nei confronti del titolare[64].
Questo modello culturale, tuttavia, non tiene conto del mutato scenario dischiuso dalle applicazioni di intelligenza artificiale che, in contrasto con il principio di minimizzazione, si avvalgono di ingenti volumi di dati, di là da ogni limite qualitativo e quantitativo di congruità funzionale minima dell'attività di trattamento e, in contrasto con il principio di limitazione della finalità, non raccolgono i dati per finalità determinate preventivamente né li trattano esclusivamente in modo non incompatibile con esse[65].
Inoltre, una gestione di tipo individuale dei dati da parte dell'interessato, che esercita un controllo in termini reattivi nel rapporto con i titolari del trattamento, appare inadeguata a offrire una tutela piena ed effettiva nei confronti dei sistemi algoritmici di elaborazione dei dati, poiché la portata discriminatoria della profilazione e delle decisioni automatizzate può prescindere dalla lesione di una posizione individuale, derivando piuttosto dall'impatto esercitato dalla sommatoria di una grande quantità di trattamenti[66].
In questa prospettiva, si osserva lo sviluppo di una *strategic litigation* che impiega il diritto antidiscriminatorio per sottoporre al sindacato giudiziale le decisioni basate sul trattamento algoritmico dei dati personali.
Emblematica appare la giurisprudenza in materia di piattaforme digitali, che affidano a un algoritmo il processo organizzativo e gestionale delle prestazioni dei lavoratori[67]. In particolare, una significativa decisione di merito ha reputato contraria al principio di non discriminazione in base alle convinzioni personali – che, secondo la Suprema Corte, "comprende anche le motivazioni e l'affiliazione sindacale"[68]– l'attività di profilazione dei

[63] Osserva G. RESTA, *op. cit.*, 226, che un notevole limite dell'approccio regolatorio del GDPR consiste «nella prevalente logica individualistica attraverso la quale ci si accosta a un tema di rilevanza decisamente meta individuale e collettiva, quale è quello delle decisioni algoritmiche».
[64] Sull'impostazione di politica legislativa del GDPR v. le lucide considerazioni di D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it.*, 2019, 2783 ss.
[65] Cfr. le considerazioni di G. FINOCCHIARO, *Intelligenza Artificiale e protezione dei dati personali*, in *Giur. it.*, 2019, 1677.
[66] Per questa ragione, secondo G. RESTA, *op. cit.*, 226, "gli strumenti di tutela, finalizzati ad assicurare un controllo esterno sulle decisioni algoritmiche, dovrebbero essere improntati ad una logica di azione *collettiva* piuttosto che individuale".
[67] La sfida posta dalla *platform economy* al diritto privato e a quello del lavoro è approfondita da D. POLETTI, *Produzione e lavoro nell'età delle piattaforme digitali*, in *Rapporti civilistici e intelligenze artificiali: attività e responsabilità*, a cura di P. Perlingieri, S. Giova e I. Prisco, Napoli, 2020, 157 ss.
[68] Così, Cass., 2 gennaio 2020, n. 1, in *Riv. it. dir. lav.*, 2020, 2, II, 377.

rider funzionale alla loro valutazione reputazionale[69]. In particolare, l'algoritmo, attribuendo una penalizzazione nel caso di cancellazione tardiva dalle sessioni di lavoro, condizionava le possibilità di accesso dei ciclo-fattorini alle sessioni successive e, dunque, alle *chance* lavorative. La cecità del sistema decisionale automatico rispetto alle motivazioni che inducano i lavoratori ad annullare senza preavviso le prenotazioni agli *slot* orari viene qualificata dal giudice bolognese come una discriminazione indiretta che, mediante un criterio apparentemente neutro, mette in una posizione di particolare svantaggio i lavoratori che si astengano legittimamente dal lavoro per esercitare il diritto di sciopero[70].
La sottoposizione dei processi decisionali automatizzati alla normativa anti-discriminatoria permette, invero, di spostare l'asse del controllo ordinamentale dal versante *soggettivo* del rispetto del diritto all'autodeterminazione informativa a quello *oggettivo* della creazione di un effetto di diseguaglianza nell'accesso a un'utilità contrattuale.
In altri termini, dinanzi agli effetti discriminatori delle decisioni algoritmiche, la normativa in tema di *data protection* persegue l'obiettivo di rendere trasparente il processo decisionale automatizzato, informando gli interessati della logica interna di funzionamento e permettendo un intervento umano, mentre quella antidiscriminatoria tende a reprimere il trattamento deteriore fondato sull'esistenza di un fattore di rischio, qualora non sia giustificato da una finalità legittima.
Sebbene la trasparenza della logica macchinica favorisca la rilevabilità dei trattamenti differenziati in base alle caratteristiche protette – quali, ad esempio, le differenziazioni di prezzo o di condizioni contrattuali – che rischierebbero altrimenti di rimanere ignoti ai consumatori, la leggibilità dell'algoritmo e l'invocabilità di una forma di partecipazione umana – comunque riferibili ai soli casi di decisioni totalmente automatiche – non sono in grado di contrastare la formazione di sub-mercati segmentati per categorie soggettive, rivelandosi inidonei a rimuovere l'incidenza dei preconcetti radicati nell'ambiente sociale sulle dinamiche di mercato[71].
Diversamente, la proibizione di discriminare costituisce un intervento eteronomo che mira a impedire proprio l'esclusione dall'accesso agli scambi contrattuali dei gruppi sociali svantaggiati[72]. Nel caso di decisioni compiute dalle intelligenze artificiali, il divieto di discriminazione, in particolar modo di quella indiretta, costituisce la tecnica di elezione per smascherare la pretesa neutralità dei parametri utilizzati dall'algoritmo, di fatto idonei a svantaggiare i componenti di un certo gruppo rispetto alla collettività[73]. Senza distinguere tra processi totalmente o parzialmente automatizzati, il sindacato giudiziale dà rilievo all'altrimenti invisibile nesso di causalità che intercorre tra un fattore di rischio e l'effetto di diseguaglianza, soggetto a una qualificazione in termini di illiceità in assenza di una

[69] Cfr. Trib. Bologna, 31 dicembre 2020, in *Nuova giur. civ. comm.*, 2021, I, 813 ss., con nota di G. PISTORE, *I* riders *e l'algoritmo. Alcune questioni in materia di discriminazione*.
[70] In questo senso, Trib. Bologna, 31 dicembre 2020, cit. Nella giurisprudenza lavoristica v., più di recente, Trib. Palermo, Sez. lav., 31 marzo 2023 e Trib. Palermo, Sez. lav., 20 giugno 2023, che hanno considerato contrarie all'art. 28 Stat. lav. le condotte di una società di consegna di cibo in rete che rifiuti di fornire alle organizzazioni sindacali le informazioni relative, rispettivamente, all'utilizzo di sistemi decisionali automatizzati e alla logica e al funzionamento dei sistemi automatizzati di gestione dei diversi aspetti del rapporto di lavoro dei *riders* e della sua cessazione, munendo la condanna dell'*astreinte* ai sensi dell'art. 614-*bis* c.p.c.
[71] Una riflessione sull'impatto delle discriminazioni algoritmiche sul funzionamento concorrenziale dei mercati in A. PEZZOLI e A. TONAZZI, *Discriminazione e collusione tacita tra lessico, intelligenza artificiale e algoritmi*, in *Analisi giur. econ.*, 2019, 201 ss.
[72] R. DI RAIMO, *Decisioni e attuazioni algoritmiche delle situazioni sostanziali*, in *Rapporti civilistici e intelligenze artificiali*, cit., 124, distingue l'incidenza dei processi decisionali algoritmici in area negoziale, con riferimento a "decisioni incidenti sull'*an*"; "decisioni esecutive in senso stretto" e "decisioni aggiudicative".
[73] In argomento, v. S. TOMMASI, *Algoritmi e nuove forme di discriminazione: uno sguardo al diritto europeo*, in *Revista de Direito Brasileira*, 2020, 27, 112 ss.

giustificazione oggettiva, consistente nel perseguimento di uno scopo legittimo che si realizzi con mezzi non sproporzionati.
La distribuzione dell'onere probatorio dell'illecito discriminatorio accentua l'incisività della tutela, configurando una presunzione legale relativa, in base alla quale il ricorrente è dispensato dalla dimostrazione del carattere ingiustificato dell'effetto di diseguaglianza, mentre il convenuto – per contestare il carattere illecito della disparità di trattamento – è tenuto a fornire la prova di una giustificazione oggettiva che superi il *test* di «proporzionalità»[74].
Pertanto, con riferimento alle discriminazioni algoritmiche consistenti nel precludere l'accesso al bene o servizio scambiato o, più frequentemente, nell'applicare prezzi e condizioni contrattuali differenziate in base a una caratteristica protetta del consumatore[75], il professionista dovrà assolvere l'onere di dimostrare che, nel singolo caso concreto, esse siano obiettivamente giustificate dal perseguimento di uno "scopo legittimo" – che, nella giurisprudenza di Lussemburgo, è una nozione da interpretarsi restrittivamente, non identificabile con il fine generico dell'incremento del profitto, ma con l'attuazione di specifiche esigenze meritevoli di tutela[76] – da conseguirsi con mezzi connotati da "appropriatezza" e "necessità", nel ragionevole bilanciamento con gli interessi in conflitto che non devono essere pregiudicati in modo sproporzionato[77].
Nello scenario dischiuso dall'applicazione di modelli algoritmici alle decisioni pubbliche e private, allora, l'applicazione del divieto di discriminazione opera come una tutela che – pur non applicandosi a ogni disparità di trattamento, come quelle legate all'impiego di un *browser* da parte del consumatore – svaluta la diffusa tendenza a incorporare, anche non intenzionalmente, i pregiudizi sociali nei dati di apprendimento che guidano le funzioni predittive, reprimendo a valle del processo di formazione della decisione i risultati finali che producano differenze di trattamento proibite[78].
Per di più, il paradigma normativo anti-discriminatorio permette di controllare le disparità generate dai sistemi di intelligenza artificiale anche quando sono aggregati ed elaborati non soltanto dati personali, ma dati non personali o informazioni anonime nei confronti dei quali il GDPR non trova applicazione[79], o quando i meccanismi di *machine learning* individuino autonomamente i parametri delle proprie decisioni, rendendo oltremodo ardua la verifica di leggibilità di una logica di funzionamento destinata a mutare in modo progressivo, mediante l'apprendimento automatico da parte dell'agente intelligente.

---

[74] Sul punto v., *amplius*, G. CARAPEZZA FIGLIA, *Il divieto di discriminazione quale limite all'autonomia contrattuale*, cit., 1412 ss.
[75] Cfr., altresì, A. NERI, *Uso di un algoritmo discriminatorio nella contrattazione privata*, in *Nuova giur. civ. comm.*, 2021, 983 ss.
[76] Si v. F.Z. BORGESIUS (a cura di), *Discrimination, Artificial Intelligence, and Algorithmic Decision-Making*, Council of Europe, Strasbourg, 2018, 19 s.
[77] Ad esempio, Corte giust., Grande Sez., 16 luglio 2015, c. 83/14, Chez c. Nikolova, ha affermato che la prassi apparentemente neutra di collocare i contatori elettrici in un quartiere urbano prevalentemente popolato da rom, su pali aerei a un'altezza di sei o sette metri, mentre tali contatori sono collocati a un'altezza inferiore ai due metri negli altri quartieri, può essere considerata dal giudice nazionale una discriminazione indiretta che comporti un particolare svantaggio per le persone di una determinata origine etnica, qualora non sia giustificata dalla volontà di garantire la sicurezza della rete di trasporto, purché non sussistano altri mezzi meno restrittivi che consentano di raggiungere dette finalità, oppure, in mancanza di essi, la misura pregiudichi in maniera sproporzionata l'interesse degli utenti ad accedere alla fornitura di energia a condizioni che non presentino carattere offensivo o stigmatizzante e permettano di controllare regolarmente il proprio consumo.
[78] Cfr. P. ZUDDAS, *Intelligenza artificiale e discriminazioni*, in Liber Amicorum *per Pasquale Costanzo*, *Consulta online*, 16 marzo 2020, 12.
[79] Il problema è affrontato da A. ASTONE, *Autodeterminazione nei dati e sistemi A.I.*, in *Contr. impr.*, 2022, 432 ss., la quale evidenza come "nel mercato dei *Big data*, esiste una contiguità tra dati personali e non personali" (p. 434).

In conclusione, in uno scenario suscettibile di essere rivoluzionato dall'approvazione dell'*Artificial Intelligence Act*, l'effettività delle tutele civili esperibili nei confronti dei trattamenti automatizzati di dati è fortemente accentuata dall'apparato rimediale offerto dalla normativa anti-discriminatoria, che arricchisce lo strumentario previsto dalla *data protection law* con tecniche di natura inibitoria, invalidante e risarcitoria in grado di contrastare la temibile incorporazione delle disparità sociali nei processi decisionali algoritmici[80].

[80] Una raffinata teorizzazione dell'effettività quale principio in grado di orientare l'interprete nella ricerca della tutela più adeguata all'interesse leso in G. VETTORI, *Effettività fra legge e diritto*, Milano, 2020.

CONSENSO AL TRATTAMENTO E GIURISPRUDENZA EUROPEA: TRA TUTELA DEI DIRITTI FONDAMENTALI E GIUSTIZIA CONTRATTUALE

Di Paola Iamiceli

SOMMARIO: 1. Il consenso al trattamento dei dati personali tra matrice costituzionale e dimensione economica. – 2. Il consenso come atto di esercizio di un diritto fondamentale. – 2.1. La libertà del consenso tra inalienabilità del diritto e nuovi orientamenti della Corte di giustizia. – 3. Il consenso al trattamento nel contesto di rapporti asimmetrici tra tutela dei diritti fondamentali e regolazione del mercato. – 4. Complementarità degli approcci e tutela effettiva dei diritti fondamentali. – 5. Alcuni rilievi conclusivi.

1. Il consenso al trattamento dei dati personali tra matrice costituzionale e dimensione economica.

Nell'esaminare la disciplina del consenso al trattamento dei dati personali attraverso la lente della giurisprudenza europea, questo contributo si interroga sulle funzioni dell'autodeterminazione dell'interessato sotto almeno due profili: (*i*) quello del consenso quale esercizio di un diritto fondamentale della persona e (*ii*) quello del consenso quale strumento di governo dei dati e meccanismo di correzione o contenimento dello squilibrio di relazioni asimmetriche nel contesto delle forme di regolazione del mercato interno. Non si affronterà invece in questa sede un terzo profilo di analisi, pur connesso e di rilievo nel quadro della recente evoluzione legislativa europea, come tale ancora estranea all'intervento della Corte di giustizia, vale a dire: (*iii*) il ruolo del consenso quale strumento propulsivo del c.d. 'altruismo' dei dati[1].

[1] Ciò nella direzione di una crescente ma governata accessibilità ai dati (anche) personali, che possa essere funzionale al loro uso (e riuso) per finalità di pubblico interesse, quali la ricerca biomedica, la lotta ai cambiamenti climatici, il miglioramento della mobilità e della fornitura dei servizi pubblici. Si tratta di materia che ha assunto rilevanza centrale negli ultimi interventi dell'Unione europea in tema di dati. Si veda in particolare il Regolamento UE/2022/868 del 30.5.2022, relativo alla *governance* europea dei dati (c.d. *Data Governance Act*), con il quale si stabiliscono (a) le condizioni per il riutilizzo, all'interno dell'Unione, di determinate categorie di dati detenuti da enti pubblici; (b) un quadro di notifica e controllo per la fornitura di servizi di intermediazione dei dati; (c) un quadro per la registrazione volontaria delle entità che raccolgono e trattano i dati messi a disposizione a fini altruistici; e (d) un quadro per l'istituzione di un comitato europeo per l'innovazione in materia di dati. L'art. 2 definisce l''altruismo dei dati' come "la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale". In un simile contesto, non solo il consenso dell'interessato vede riaffermato il proprio ruolo (v. Considerando (50)), ma il Regolamento traccia la strada per la definizione di un modello europeo di consenso all'altruismo dei dati valido in tutti gli Stati membri e rispettoso dei principi del Regolamento Generale dei Dati (v. art. 25 Reg. UE/2022/868). Sul tema, G. RESTA, *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl.*, 2022, 971 ss.; S. ORLANDO, *Il coordinamento tra la Direttiva 2019/770 e il GDPR. L'interessato-consumatore*, in *Pers. merc.*, 2023, 222.

È ormai difficilmente contestabile che, pur rappresentando il tratto distintivo della disciplina europea dei dati nel panorama globale, la tutela dei diritti fondamentali non sia ormai l'unico punto di osservazione di tale disciplina[2]. Del resto, pur fornendo ormai l'art. 16 TFUE, una distinta base giuridica all'intervento legislativo dell'Unione in tema di protezione dei dati personali, i primi considerando e i primi articoli del Regolamento Generale sulla Protezione dei Dati (di qui in avanti, GDPR o Regolamento) chiariscono in modo esplicito la connessione esistente tra tutela dei diritti fondamentali e istanze di circolazione dei dati, in quanto funzionali al buon funzionamento del mercato interno[3]. Non a caso al Regolamento si assegna, *ex* art. 1, la duplice finalità di protezione delle persone fisiche con riguardo al trattamento dei loro dati personali e di garanzia della circolazione di tali dati, precisandosi che la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali[4].
Tanto più alla luce dei recenti interventi legislativi in ambito europeo[5], assume dunque particolare rilievo la stretta correlazione tra la dimensione, per così dire, costituzionale (legata al paradigma dei diritti fondamentali) e la dimensione, *lato sensu*, economica (legata alla circolazione dei dati connessa, in ultima analisi e comunque prevalentemente, al funzionamento del mercato). Esaminare le implicazioni di questa correlazione nell'ambito della giurisprudenza europea sul consenso al trattamento è tra gli obiettivi di questa breve riflessione, con la quale si proverà ad articolare alcune considerazioni preliminari in tema di tutela effettiva dell'interessato a cavallo tra disciplina dei dati personali e disciplina consumeristica[6].

2. Il consenso come atto di esercizio di un diritto fondamentale

Che il consenso al trattamento dei dati personali sia parte del diritto fondamentale alla protezione dei dati personali lo si desume dall'art. 8 della Carta dei diritti fondamentali dell'Unione. Non solo l'art. 8 configura tale consenso come atto in sé idoneo a rappresentare un 'fondamento legittimo' del trattamento dei dati personali[7] ma è proprio sul consenso che la

[2] V. G. RESTA, *op. ult. cit.*, 974 ss., dove si mette in luce il passaggio da un modello unipolare, dominante da oltre cinquant'anni e incentrato sulla tutela dei dati personali come diritto fondamentale, a un modello multipolare, oggi accolto dal *Data Governance Act* e dal *Data Act*, volto a considerare di pari dignità le istanze connesse a tale tutela e quelle di libero accesso e riuso dei dati (anche personali).
[3] Si vedano in particolare i Considerando 1, 5, 9, Regolamento Generale sulla Protezione dei Dati.
[4] Così il terzo comma dell'art. 1 GDPR. Che il Regolamento da solo tenga sempre conto di questo bilanciamento, dettando disposizioni che siano in concreto funzionali alla circolazione dei dati oltre che alla tutela dei diritti fondamentali, è oggetto di dibattito (e talora di critiche). Ne dà conto G. RESTA, *op. ult. cit*.
[5] A partire dalla non più recente dir. 2019/770/UE sulla tutela consumeristica nei contratti aventi ad oggetto contenuti e servizi digitali, in cui la correlazione tra tutela dei dati personali e funzionamento del mercato è al centro dell'intervento legislativo dell'Unione. V. G. RESTA, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva UE 2019/770 e il Regolamento UE/2016/679*, in *Ann. Contr.*, 2018, 125 ss.; C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in *Giust. civ.*, 2019, 499 ss.; S. ORLANDO, *op. cit*.
[6] Nella prospettiva tracciata, sulla scia degli studi di N. Reich (ID., *General Principles of EU Civil Law*, CUP, Cambridge, 2013) da G. Vettori in ID., *Effettività delle tutele (diritto civile)*, in *Annali Enc. dir.*, Milano, 2017, 381 ss., 394 ("la Corte [di giustizia] utilizza l'effettività come un principio costituzionale con precise finalità: (a) eliminare le restrizioni nazionali nella protezione dei diritti; (b) potenziare la funzione ermeneutica; (c) individuare i rimedi più adeguati alla lesione"); poi sviluppata in ID., *Effettività tra legge e diritto*, Milano, 2020, 105 ss.
[7] Chiaramente la legittimità del fondamento dipende dalla legittimità del consenso (in ragione della conformità alle norme che lo regolano) e dalla sua liceità (in ragione della sua non contrarietà a norme imperative, di ordine pubblico e buon costume, altrimenti desumibili dall'ordinamento). V. S. ORLANDO, *Per un sindacato di liceità del consenso* privacy, in *Pers. merc.*, 2022, 527 ss.

norma fa leva per ascrivere la protezione dei dati personali al novero delle 'libertà', quali delineate nel titolo II della Carta[8].
Là dove l'art. 7 Direttiva CE/95/46 qualificava il consenso come presupposto di legittimazione del trattamento, scindendo (forse solo apparentemente) lo statuto della legittimità da quello della liceità *ex* art. 6 della medesima Direttiva, il GDPR associa espressamente liceità del trattamento e definizione delle basi giuridiche dello stesso, assegnando all'art. 6, in tema di liceità, quella funzione di bilanciamento tra interessi, individuali, collettivi e pubblici, che è tipica della disciplina dei diritti fondamentali. In questo contesto, è il consenso dell'interessato a 'svettare' tra le basi giuridiche del trattamento: tra tutte, è infatti pressoché l'unica a coniugare protezione dei dati personali e autodeterminazione dell'interessato, lasciando in sostanza a quest'ultimo la funzione di bilanciamento tra interessi che, rispetto alle altre basi giuridiche, è affidata al legislatore e poi all'autorità di controllo e al giudice[9]. Come opportunamente osservato in dottrina, ciò non esclude che la valutazione della liceità del consenso (quale presupposto della – diversa – liceità del trattamento) possa richiedere un ulteriore bilanciamento di interessi, quando ad esempio il trattamento a cui si acconsente è di per sé funzionale all'esercizio di un'attività illecita, lesiva di interessi dell'interessato o di terzi[10].
Alla dimensione costituzionale del consenso come esercizio di un diritto fondamentale all'autodeterminazione sono riconducibili le affermazioni dell'Avvocato Generale Szpunar nel caso *Orange v. Romania*, là dove si afferma che il "consenso consente alla persona interessata di decidere personalmente circa la legittimità delle restrizioni al suo diritto alla protezione dei dati personali" e che "il principio cardine su cui si fonda il diritto dell'Unione in materia di protezione dei dati è quello di una decisione di una persona fisica autodeterminata in grado di compiere scelte riguardanti l'uso e il trattamento dei suoi dati"[11]. E in analoga prospettiva sembra doversi leggere l'orientamento della Corte di giustizia incline a un'interpretazione restrittiva delle basi giuridiche diverse dal consenso, come se in tali casi si determinasse una deviazione dalla strada maestra, evidentemente ancorata alla base giuridica consensualistica quale espressione di un diritto fondamentale: in quanto eccezioni alla regola, le norme relative alle basi giuridiche diverse dal consenso vanno interpretate in senso restrittivo[12]. Rientra in questa logica restrittiva una lettura delle norme circa le basi non consensualistiche del trattamento rivisitata alla luce del principio di affidamento[13].

---

[8] V. le Conclusioni dell'Avvocato Generale M. Szpunar, 4.3.2020, C-61/19, *Orange v. Romania*, ECLI:EU:C:2020:158, par. 36: "Il requisito del consenso della persona interessata è una caratteristica essenziale sottesa al diritto dell'Unione sulla protezione dei dati. Esso figura nella Carta dei diritti fondamentali dell'Unione europea, in cui si stabilisce, all'articolo 8, che i dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge".
[9] Questo è solo in parte vero con riferimento all'ipotesi in cui il trattamento dei dati personali è necessario all'esecuzione del contratto (ex art. 7, comma 1, lett. *b*). Sebbene in tal caso la necessarietà sia da valutarsi in senso puramente oggettivo e a prescindere da qualsiasi presa di coscienza da parte dell'interessato, non si può del tutto escludere una partecipazione di quest'ultimo alla determinazione relativa al trattamento dei dati e dunque alla valutazione degli interessi in gioco (cfr. Corte giust. UE, 4.7.2023, *Meta Platforms*, C-252/21, ECLI:EU:C:2023:537, par. 98 e 99).
[10] S. ORLANDO, *op. cit.*, 527 ss., part. 537. Sul rapporto tra liceità del trattamento e bilanciamento tra interessi, sia consentito il rinvio a P. IAMICELI, *Liceità, correttezza, finalità nel trattamento dei dati personali*, in *Diritto alla riservatezza e circolazione dei dati personali*, a cura di R. Pardolesi, Milano, 2000, I, 395 ss., spec. 408 ss.
La necessità di una duplice valutazione di liceità emerge anche in relazione all'assunzione di decisioni automatizzate, dovendosi distinguere tra liceità del consenso al trattamento dei dati strumentale al processo di decisione automatizzata e liceità del consenso all'automatizzazione della decisione *ex* art. 22 GDPR. Sui requisiti di validità di quest'ultimo alla luce dei principi di razionalità e non discriminazione, si veda D. IMBRUGLIA, *Le presunzioni delle macchine e il consenso dell'interessato*, in *Riv. trim. dir. proc. civ.*, 2023, 921 ss.
[11] V. Conclusioni dell'Avvocato Generale M. Szpunar, *Orange v. Romania*, C-61/19, cit., parr. 36 e 37.
[12] Corte giust. UE, *Meta Platforms*, C-252/21, cit., par. 92 e 93.
[13] Corte giust. UE, *Meta Platforms*, C-252/21, cit., par. 117: "A tal riguardo, occorre rilevare che, malgrado la gratuità dei servizi di un social network online quale Facebook, l'utente di quest'ultimo non può ragionevolmente

Secondo un'impostazione che può essere considerata distintiva dell'approccio europeo, la matrice costituzionale del consenso come strumento di esercizio di una libertà di autodeterminazione ne ha segnato la disciplina, tanto con riguardo ai criteri di valutazione di integrità del volere, quanto con riferimento al rapporto tra consenso e contratto[14].
Proprio in quanto connessa all'esercizio di una libertà fondamentale, la natura libera, informata, manifesta, specifica del consenso al trattamento non permette di assimilarne i requisiti di validità a quelli propri di qualsiasi atto di autonomia privata[15]. Diversamente da questi, essa deve farsi carico di quel principio di effettività della tutela dei diritti fondamentali che, sebbene contemperato dal principio di proporzionalità, finisce per spostare l'ago della bilancia a favore dell'interessato, anche quando l'affidamento del titolare o del responsabile del trattamento possa risultarne in qualche modo pregiudicato.
Si comprende allora perché, ad esempio, non basti che il consenso segua le sorti dei contratti per adesione, per cui, *ex* art. 1341, co. 1, c.c., la determinazione contrattuale produce effetti tra le parti in base alla mera conoscibilità da parte del non predisponente: nella lettura della Corte di giustizia, serve invece che il consenso si àncori a una determinazione "effettivamente letta e assimilata"[16], ben più che conosciuta o conoscibile. Anche di recente (e con ulteriore enfasi data dalla natura potenzialmente sensibile dei dati trattati) la Corte ha sottolineato l'importanza di un consenso prestato "con piena cognizione di causa", con particolare riferimento alla consapevolezza circa le finalità del trattamento e l'accessibilità più o meno diffusa dei dati trattati da parte del pubblico[17]. La natura inequivocabile della manifestazione del consenso, sottolinea ancora il giudice europeo, esclude la rilevanza di un consenso sotteso a un comportamento passivo, implicito, per fatto concludente, richiedendo invece un'attiva e

attendersi che, senza il suo consenso, l'operatore di tale social network tratti i suoi dati personali a fini di personalizzazione della pubblicità. In tali circostanze, si deve ritenere che i diritti fondamentali e gli interessi di tale utente prevalgano sull'interesse dell'operatore a tale personalizzazione della pubblicità mediante la quale egli finanzia la sua attività, cosicché il trattamento da quest'ultimo effettuato a tali fini non può rientrare nell'ambito di applicazione dell'articolo 6, paragrafo 1, primo comma, lettera f), del RGPD".

[14] Gli studi di diritto comparato tendono a mettere in luce i diversi approcci sulle due rive dell'Atlantico, valorizzando la matrice costituzionale dei diritti della personalità, prevalentemente incentrata sulla dignità della persona nel vecchio continente in contrapposizione a una lettura nordamericana prevalentemente incentrata sul paradigma della libertà, quale libertà dallo Stato. Su questo confronto, anche in chiave storica e sociologica, J. Q. WHITMAN, *The Two Western Cultures of Privacy: Dignity versus Liberty*, in *Yale Law Journal*, 2004, 1151-1221; con riferimento alla più recente evoluzione del diritto nordamericano: W. HARTZOG e N. RICHARDS, *Privacy's Constitutional Moment and the Limits of Data Protection*, in *B.C.L. Rev.*, 2020, 1687. Per una più ampia analisi comparatistica v. M. J. CEPEDA ESPINOSA, *Privacy*, in *The Oxford Handbook of Comparative Constitutional Law*, a cura di M. Rosenfeld e A. Sajò, Oxford University Press, Oxford, 2012, 866 ss., spec. 968 ("the idea of privacy is context-bound and linked to culture").

[15] V. Cass. civ., sez. I, 2.7.2018, n. 17278, par. 2.4 ("è anzitutto da escludere che il consenso considerato da tale disposizione sia semplicemente il medesimo consenso in generale richiesto a fini negoziali, ossia il consenso prestato da un soggetto capace di intendere e volere e non viziato da errore, violenza o dolo, ovvero, in determinati frangenti, da pericolo o da bisogno: consenso, quello così previsto, che pur sussiste quantunque perturbato, al di sotto di una determinata soglia, in ragione dei vizi indicati, secondo quanto risulta dagli artt. 1428, 1435 e 1439 c.c."), in *GiustiziaCivile.com*, con nota di F. RUGGERI, *Sulla nozione di consenso nella nuova disciplina privacy: alcune prime considerazioni*. Sulla distinzione e il rapporto tra consenso contrattuale e consenso negoziale, pur da diverse prospettive, G. RESTA, *op. cit.*, 144 s.; C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770*, cit.; S. PAGLIANTINI, *Sul negozio giuridico. Itinerari novecenteschi e della contemporaneità*, Napoli, 2023, 30 ss. (dove si riconosce la natura negoziale del consenso); S. ORLANDO, *Il coordinamento tra la Direttiva 2019/770*, cit., 231, dove, superandosi la tesi della duplicità degli atti di autonomia (l'adesione al contratto e il consenso al trattamento), si configura l'esistenza di un'unica 'manifestazione della volontà contrattuale rafforzata, a cui si applicano prioritariamente le norme sulla protezione dei dati personali e, per quanto compatibili, quelle sul contratto.

[16] Corte giust. UE, 11.11.2020, *Orange v. Romania*, C-252/21, ECLI:EU:C:2020:901, par. 46.

[17] Corte giust. UE, *Meta Platforms*, C-252/21, cit., par. 82.

manifesta presa di posizione da parte dell'interessato[18]. Da ciò deriva anche la sua specificità e dunque l'impossibilità di desumere il consenso da atti di autonomia che a quel consenso sono soltanto connessi (es. la richiesta di un servizio), tanto più che, come tutte le basi giuridiche, il consenso è correlato a determinate finalità del trattamento, imponendosi dunque, anche sotto questo profilo, la sua specificità[19].

2.1. La libertà del consenso tra inalienabilità del diritto e nuovi orientamenti della Corte di giustizia

Tra tutti quelli sopra richiamati, l'elemento che maggiormente riflette la natura del consenso come meccanismo di autodeterminazione ed espressione di un diritto fondamentale è senza dubbio la 'libertà' del suo esercizio. Tanto nel Regolamento, quanto nella giurisprudenza europea, tale libertà è declinata nel senso di una sottrazione dell'interessato a condizionamenti esterni. È ispirata a un principio di effettività della scelta, che, in quanto libera, deve lasciare aperta la strada del diniego del trattamento dei dati personali non giustificato da basi giuridiche diverse dal consenso.
È questo un profilo molto complesso, in relazione al quale si confrontano posizioni e sensibilità assai diverse non solo nel dibattito scientifico, ma anche nel dialogo giurisdizionale. L'assenza di condizionamenti esterni corre infatti lungo una linea molto sottile, che separa i fattori determinanti di una scelta comunque 'libera' e quelli condizionanti una scelta non più tale. In un contesto in cui, sul piano funzionale, il dato personale incorpora ormai un valore economico idoneo a farne strumento di remunerazione, ancorché parziale, nello scambio di beni e servizi sul mercato, la libertà di scelta dell'interessato si dissocia con difficoltà dalla "scelta di natura commerciale"[20], scelta che lo stesso interessato compie spesso contestualmente alla manifestazione del consenso al trattamento dei dati personali.
Messa da parte l'ipotesi in cui il trattamento dei dati assolva una funzione del tutto strumentale all'esecuzione del contratto (rendendo dunque irrilevante la prestazione del consenso, in presenza della diversa base giuridica di cui all'art. 6, § 1, lett. b, GDPR), la questione è se e quando il consenso al trattamento di dati personali per altre finalità (peraltro necessariamente dichiarate) possa dirsi libero quando, per scelta commerciale, l'operatore subordini ad esso la prestazione del servizio stesso.
Data la complessità della questione, non sorprende che, lungi da instaurare difficili automatismi, il legislatore europeo si limiti a mettere in guardia l'interprete, stabilendo 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, § 4, GDPR, corsivo nostro). Può essere utile aggiungere che, nel tentativo di far chiarezza, il Comitato Europeo per la Protezione dei Dati ha affermato che tale condizionamento deve essere valutato tenendo conto della possibilità, concessa dal titolare del trattamento, di accedere a servizi "effettivamente

[18] V., con riferimento all'art. 4, § 11, GDPR (e alla disposizione corrispondente già contenuta nella Direttiva 95/46/UE), Corte giust. UE, 19.10.2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, par. 52; Corte giust. UE, *Orange v. Romania*, C-252/21, cit., par. 35-36.
[19] Corte giust. UE, *Planet49*, cit., par. 58; Corte giust. UE, *Orange v. Romania*, cit., par. 38. Sulla specificità del consenso rispetto ai singoli trattamenti di pertinenza di ciascun titolari, v. anche, in presenza di più titolari, Corte giust. UE, 29.10.2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, par. 102 ss.
[20] Questo il lemma usato dal legislatore europeo nella Dir. 2005/29/CE in tema di pratiche commerciali scorrette (v. art. 2, lett. k).

equivalenti" senza la prestazione del consenso[21]. L'interessato non sarebbe infatti libero nella sua autodeterminazione se fosse indotto al consenso dalla necessità di accedere al servizio e dall'impossibilità di farlo (in modo 'equivalente', appunto) se non acconsentendo al trattamento dei dati[22].
Due questioni paiono allora affacciarsi: (*i*) se l'assenza di un'opzione alternativa configuri in sé un condizionamento tale da rendere il consenso prestato necessariamente non libero; (*ii*) se un'alternativa al servizio abbinato alla prestazione del consenso, che consista in un servizio del tutto omologo a quello offerto ma associato a condizioni di prezzo diverse (per cui il servizio diventi oneroso o lo sconto applicato in ipotesi di consenso si riduca o si elimini), possa dirsi 'equivalente' ai sensi delle Linee Guida del Comitato[23].
Sotto il primo profilo giova ricordare che, nell'art. 7, § 4 già richiamato, il GDPR non vieta di configurare il consenso come condizione per l'accesso al servizio, ma impone in questa ipotesi una più rigorosa valutazione della sua effettiva libertà[24].
Nella medesima direzione sembra del resto potersi leggere una nota decisione della Corte di cassazione, che, al fine di salvaguardare la piena libertà del consenso prestato nelle circostanze sopra dette, guarda alla natura del servizio 'condizionato' in quanto "infungibile e irrinunciabile per l'interessato"[25]. Nella prospettiva della Suprema Corte, il consenso prestato al fine di accedere a un servizio non sostituibile né rinunciabile (si pensi a un servizio educativo o a un servizio sanitario personalizzato, per i quali non esista nel mercato un'alternativa ugualmente soddisfacente per l'interessato) non può dirsi libero. A ben guardare, sembra così indirettamente ammettersi che il consenso possa essere libero se l'interessato abbia (consapevolmente, si intende) acconsentito al trattamento di dati, pur non necessari all'esecuzione del contratto, ove costui possa comunque accedere al servizio ricorrendo ad altri operatori (trattandosi di servizio fungibile)[26] o addirittura rinunciarvi (essendo il servizio non essenziale). Emerge in questa sede un'importante correlazione tra libera autodeterminazione

---

[21] Comitato Europeo per Protezione dei Dati (CEPD), *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, 4.5.2020, 12, par. 37.
[22] Il criterio di equivalenza torna anche nel linguaggio del legislatore europeo nel Regolamento 2022/1925/UE relativo a mercati equi e contendibili nel settore digitale (regolamento sui mercati digitali), Considerando 36 e 37. Sul tema di veda oltre nt 47 e testo corrispondente.
[23] Le due questioni riflettono, in altra prospettiva, gli sviluppi del caso *Meta* esaminati nel procedimento C-252/21, conclusosi di recente con la sentenza della Corte di giustizia, già citata. In una prima fase l'Autorità federale tedesca garante della concorrenza aveva vietato a Meta Platforms di subordinare, nelle sue condizioni generali, l'uso del social network da parte di utenti privati residenti in Germania al trattamento di alcuni dati personali. Ad esito di tale provvedimento Meta ha introdotto nuove condizioni generali le quali indicano espressamente che l'utente dichiara di acconsentire alle inserzioni pubblicitarie (previo trattamento di dati personali dell'utente) "invece di pagare per l'uso dei servizi Facebook".
[24] G. RESTA, *op. cit.*, 139.
[25] Cass. civ., sez. I, 2.7.2018, n.17278, cit., par. 2.5: "Ritiene la Corte, nel quadro di applicazione del citato art. 23, che la risposta al quesito non possa essere univoca e, cioè, che il condizionamento non possa sempre e comunque essere dato per scontato e debba invece essere tanto più ritenuto sussistente, quanto più la prestazione offerta dal gestore del sito Internet sia ad un tempo infungibile ed irrinunciabile per l'interessato, il che non può certo dirsi accada nell'ipotesi di offerta di un generico servizio informativo del tipo di quello in discorso, giacché all'evidenza si tratta di informazioni 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".
[26] Esclude che il consenso sia libero in questa circostanza il Comitato Europeo per la Protezione dei Dati nelle *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, cit., par. 38 ("Il Comitato ritiene che il consenso non possa considerarsi prestato liberamente se il titolare del trattamento sostiene che esiste la possibilità di scegliere tra il suo servizio che prevede il consenso all'uso dei dati personali per finalità supplementari, da un lato, e un servizio equivalente offerto da un altro titolare del trattamento, dall'altro. In 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 (…)").

dell'interessato e tutela di altri diritti e libertà fondamentali connessi all'accessibilità di servizi essenziali[27].
Sotto il secondo profilo, la questione appare ulteriormente controversa. Nel caso in cui il titolare prospetti un'alternativa offrendo un servizio alternativo a quello condizionato alla prestazione del consenso, può dirsi 'equivalente' quel servizio a cui è associato il pagamento di un prezzo in denaro, se il servizio originariamente offerto è gratuito, o il venir meno di uno sconto, se oneroso?
È proprio qui che la linea di confine tra condizionamenti ammessi e condizionamenti non ammessi pare rivelare tutta la sua criticità. Se si adottasse un approccio prettamente di mercato e si tenesse conto del valore economico, ormai acclarato, dei dati personali, la questione posta andrebbe sciolta in modo piuttosto semplice, ammettendosi che, una volta chiarite in modo trasparente le alternative commerciali offerte all'interessato, quest'ultimo possa scegliere, in modo libero, secondo le proprie preferenze. Anche in questa prospettiva, come sarà chiarito oltre, occorrerebbe assicurare che le condizioni economiche dell'offerta alternativa non siano tali da eliminare sostanzialmente lo spazio di scelta dell'interessato (nel qual caso si tornerebbe alla questione sub (*i*)), ma in ogni caso si ammetterebbe un consenso libero pur in presenza di un'alternativa 'equivalente' dal punto di vista del contenuto del servizio, ma non delle sue condizioni economiche.
Il RGPD parrebbe puntare in altra direzione là dove nel Considerando 42 afferma che "[i]l consenso non dovrebbe essere considerato liberamente prestato se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio", dovendosi forse intendere per 'pregiudizio' anche un pregiudizio meramente economico.
Alla luce di questa precisazione, ci si chiede se un approccio più rigoroso, volto ad escludere la libertà del consenso là dove l'alternativa esista ma sia onerosa (o più onerosa), sia allora più coerente con la natura fondamentale del diritto all'autodeterminazione[28]. Senz'altro è più coerente con quelle letture della disciplina del consenso che negano la funzione remuneratoria

[27] La questione è venuta all'attenzione dei giudici anche nel contesto pandemico, là dove i cittadini sono stati chiamati a pronunciarsi sul trattamento di dati personali (anche sensibili) ai fini del tracciamento attraverso l'iscrizione a piattaforme digitali, per poter accedere a luoghi pubblici o a servizi, alcuni dei quali essenziali. In un simile contesto preme segnalare che, con riguardo a servizi essenziali quali quelli sanitari, è probabile che, in luogo del consenso, venga in rilievo una diversa base giuridica del trattamento, es. ai sensi dell'art. 6, § 1, lett. d) o e), o, per i dati sensibili, dell'art. 9, § 2, lett. g), h) e i), GDPR. In giurisprudenza, v. Corte giust. UE, 5.10.2023, C-659/22, *Ministerstvo zdravotnictví*, ECLI:EU:C:2023:745, dove si afferma che il GDPR trova applicazione nell'ambito dei meccanismi di verifica della certificazione della vaccinazione contro il COVID-19; e, precedentemente, Corte giust. UE, ord. Pres. Tribunale, 30.11.2021, T-710/21 R, in cui si conferma la decisione del Parlamento di imporre l'esibizione del COVID pass in quanto non risulta provata, da parte dei ricorrenti, la violazione del diritto alla protezione dei dati personali. Per altri riferimenti alla giurisprudenza nazionale e sovranazionale in diversi paesi del mondo sull'impatto delle misure antipandemiche sui diritti fondamentali, inclusa la protezione dei dati personali, sia consentito il rinvio al Database "Covid19 Litigation", disponibile sul sito https://www.covid19litigation.org/, realizzato nell'ambito di un progetto co-finanziato e co-disegnato dall'Università di Trento con l'Organizzazione Mondiale della Sanità tra il 2020 e il 2023. In tema di protezione dei dati si segnalano in particolare: per Israele, Corte Suprema, 1.3.2021, HCJ 6732/20, https://www.covid19litigation.org/case-index/israel-supreme-court-israel-sitting-high-court-justice-hcj-673220-2021-03-01; per la Slovenia, Corte cost., 14.4.2022, https://www.covid19litigation.org/news/2022/05/slovenia-government-decrees-imposing-health-passes-not-constitutional-court-holds, dove si dichiarano i decreti che impongono l'esibizione del COVID pass incostituzionali e contrari al GDPR. Sul tema si consenta il rinvio a P. IAMICELI e F. CAFAGGI, *COVID-19 Litigation. The Role of National and International Courts in Global Health Crises*, Trento, 2024, disponibile su https://hdl.handle.net/11572/406169.
[28] Così, C.A. ANGIOLINI, *Lo statuto dei dati personali, Uno studio a partire dalla nozione giuridica di bene*, Torino, 2020, 126 ss., spec. 130.

del dato (non riducibile a 'merce')[29] e riconoscono nel denaro un 'condizionamento' non ammissibile secondo la logica della non alienabilità (in senso lato) degli attributi fondamentali della persona[30].
Ciò considerato in via di prima ipotesi e pur restando nel perimetro di un diritto europeo permeato dalle istanze di tutela dei diritti fondamentali, occorre tuttavia osservare come il dato positivo non porti a suffragare la tesi restrittiva appena formulata. Se la posizione del Comitato Europeo per la Protezione dei Dati (CEPD) sembra escludere il paradigma dello scambio tra dati e servizi, non può sfuggire che lo stesso legislatore europeo abbia configurato (e regolato) contratti di scambio in cui i dati assolvono o concorrono alla funzione remuneratoria intrinseca allo scambio[31]. In particolare, secondo una attenta dottrina[32], deve senz'altro ammettersi una funzione *lato sensu* remuneratoria del dato personale, fondata su un consenso libero, quando tale funzione sia associata, non all'interesse a un mero risparmio di spesa da parte dell'interessato (che potrebbe non esserci), bensì al perseguimento di altro e distinto interesse (lecito), es. a una comunicazione personalizzata, a certi contenuti digitali, a rimanere in e a non essere esclusi da un certo ecosistema digitale[33]. Questa lettura ha il merito di riuscire a coniugare libertà del consenso, autodeterminazione informativa e funzione remuneratoria del dato, nonché quello di sottolineare le opportune differenze tra funzione remuneratoria del denaro e funzione remuneratoria del dato, da correlare, quest'ultima, non a valori prettamente monetari ma a interessi di tipo sociale o culturale, se non addirittura a vere e proprie forme di altruismo.

---

[29] Cfr. Comitato Europeo per la Protezione dei Dati, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, 4.5.2020, 10 ss. (v. part. par. 35, dove si sottolinea l'eccezionalità delle situazioni in cui il consenso possa dirsi libero benché condizionante l'accesso al servizio offerto dall'operatore); v., secondo una formulazione lungamente discussa e da molti considerata di valore prettamente simbolico (così G. RESTA, *op. cit.*, 132), Cons. 24, Direttiva (UE) 2019/770: "La fornitura di contenuti digitali o di servizi digitali spesso prevede che, quando non paga un prezzo, il consumatore fornisca dati personali all'operatore economico. Tali modelli commerciali sono utilizzati in diverse forme in una parte considerevole del mercato. Oltre 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".
Sulla configurazione del contratto per la fornitura di beni o servizi "verso" dati personali alla stregua di un contratto gratuito (nell'ambito della c.d. 'gratuità interessata') a cui si affianchi, non in funzione corrispettiva, il consenso al trattamento dei dati personali, C. CAMARDI, *op. cit.*, 499 ss., che si sofferma altresì sulla correlata distinzione tra consenso contrattuale e consenso al trattamento dei dati personali. In questa prospettiva anche C.A. ANGIOLINI, *op. ult. cit.*, 208 ss.

[30] Questa impostazione trova una qualche eco nell'approccio fondato sulle c.d. 'inalienability rules' discusse nella prospettiva di *law and economics*, su cui v. S. ROSE-ACKERMAN, *Inalienability and the Theory of Property Rights*, in *Col. L. Rev.*, 85, 5, 1985, 931-969. Sul tema, muovendo dalla prospettiva dei diritti fondamentali e da un excursus storico delle regole di c.d. inalienabilità dei diritti della personalità, G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, 113 ss., 250 ss., 334 ss., dove, per un verso, si conferma il principio cardine dell'inalienabilità come principio cardine a tutela dell'autodeterminazione e della dignità dell'avente diritto e, per l'altro, si individua nel contratto con effetti derivativi-costitutivi l'atto di disposizione dei diritti della personalità. Sulla rilevanza della gratuità degli atti di disposizione del proprio corpo, come tale non estendibile al regime del consenso al trattamento dei dati personali, v., in prospettiva di diritto UE, ID., *Autonomia contrattuale e diritti della persona nel diritto UE*, in *Dig. Disc. Priv.*, sez. civ., Agg, 2013, 92 ss., 96.

[31] A. DE FRANCESCHI, *European Contract Law and the Digital Single Market: Current Issues and New Perspectives*, in *European Contract Law and the Digital Single Market*. *The implications of the Digital Revolution*, a cura di A. De Franceschi, Intersentia, Cambridge-Antwerp-Portland, 2016, 1 ss., 5; V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ.*, 2020, 3, 642 ss.; più diffusamente, ID. *L'equivoco della privacy*, Napoli, 2022, 166 ss., 168; S. ORLANDO, *Il coordinamento tra la Direttiva 2019/770*, cit.

[32] S. ORLANDO, *Per un sindacato di liceità del consenso privacy*, cit., 532.

[33] S. ORLANDO, *op. ult. cit*., 532, dove si ha riguardo all'interesse a una comunicazione personalizzata, a certi contenuti digitali, a rimanere e non essere esclusi da un certo ecosistema digitale.

Nella direzione dell'ammissibilità di un consenso libero quand'anche associato a un'alternativa onerosa, muove del resto espressamente la Corte di giustizia in una recente decisione. Probabilmente animata da un'esigenza di realismo (e forse ispirata dai più recenti orientamenti emersi nel quadro regolatorio europeo, oggi orientato a una maggiore spinta alla circolazione dei dati), la Corte finisce infatti per ammettere la libertà del consenso prestato in presenza di un'alternativa onerosa; ciò in particolare quando l'interessato abbia la possibilità di negare il consenso accettando al contempo di rinunciare 'non integralmente' al servizio e di accedere a un'alternativa equivalente "se del caso a fronte di un adeguato corrispettivo"[34].
Se dunque il paradigma dell'autodeterminazione informativa come diritto fondamentale ha consentito al legislatore e al giudice europeo di rafforzare la matrice volontaristica del consenso, presidiandone i requisiti di integrità, autenticità, consapevolezza e, in ultimo, di effettiva libertà, non mancano, specie nella legislazione e nella giurisprudenza più recenti, i segni di una rivisitazione del ruolo del consenso. Ne risulta un diverso equilibrio tra tutela dell'interessato e circolazione dei dati, che, favorendo quest'ultima, fa leva su un'idea di consenso più incline a incorporare la dimensione economica sottesa a quella circolazione.
Questo mutamento di prospettiva induce a guardare con maggiore attenzione i punti di intersezione tra tutela dei dati personali e tutela consumeristica[35]. È evidente infatti che, pur ammettendosi un consenso liberamente prestato a fronte di alternative commerciali non equivalenti sul piano del prezzo, l'effettiva libertà dell'interessato può essere assicurata solo in presenza di un'idonea prospettazione delle diverse alternative e di una piena informazione circa le finalità del trattamento in questo modo autorizzato. Tale circostanza che, secondo il Regolamento, compete al titolare provare[36], induce a spostare l'attenzione dal processo decisionale dell'interessato alla pratica del titolare, secondo una logica che il diritto europeo ben conosce nel contesto della tutela consumeristica. Ed è per questo che, nella parte che segue, ci si soffermerà sui rapporti tra tutela del diritto fondamentale all'autodeterminazione e regolazione dei rapporti economici di tipo asimmetrico, quali sono, nella maggior parte dei casi, quelli tra titolari del trattamento e singoli interessati.

3. Il consenso al trattamento nel contesto di rapporti asimmetrici tra tutela dei diritti fondamentali e regolazione del mercato

L'analisi sopra svolta mostra come, pur distintivo dell'approccio europeo nel quadro globale, il paradigma dei diritti fondamentali non sia del tutto esplicativo del sistema di regole sul consenso al trattamento quale esso si è sviluppato, nel dialogo tra corti nazionali e giudice europeo, nella giurisprudenza della Corte di giustizia.
Pare infatti chiaro che, soprattutto nella giurisprudenza più recente, le istanze di salvaguardia dell'integrità del volere, poste alla base dell'esercizio della libera autodeterminazione

[34] Corte giust. UE, *Meta Platforms*, C-252/21, cit., par. 150: "(…) tali utenti devono disporre della libertà di rifiutare individualmente, nell'ambito della procedura contrattuale, di prestare il loro consenso a operazioni particolari di trattamento di dati non necessari all'esecuzione del contratto, senza essere per questo tenuti a rinunciare integralmente alla fruizione del servizio offerto dall'operatore del social network online, il che implica che a detti utenti venga proposta, se del caso a fronte di un adeguato corrispettivo, un'alternativa equivalente non accompagnata da simili operazioni di trattamento di dati".
[35] P. IAMICELI, F. CAFAGGI e A. ANGIOLINI (a cura di), *Casebook Effective Data Protection and Fundamental Rights*, Roma, 2022, disponibile su https://www.fricore.eu/content/materials, 215 ss. Cfr. S. PAGLIANTINI, *op. cit.*, 41, dove, riconosciuto che lo scambio di dati personali quale controvalore economico di una fornitura è "retto dal baluardo di un consenso negoziale", individua nella disciplina del negozio uno strumento di riequilibrio della libertà di autodeterminazione economica del singolo di fronte al potere del professionista: "la tutela da una, cioè il GDPR, qui diventano due".
[36] Corte giust. UE, *Meta Platforms*, C-252/21, cit., 152.

informativa, finiscano per essere contemperate con esigenze di circolazione dei dati legate al buon funzionamento del mercato più che al bilanciamento con altre libertà e diritti fondamentali. Sotto questo profilo, la tutela dei dati personali, quale diritto fondamentale, si combina con logiche regolatorie del mercato e tiene conto dei fallimenti tipici dell'autonomia privata indotti dalle asimmetrie informative e di potere negoziale tipiche di alcune relazioni di mercato.

La complementarità tra tutela dei diritti fondamentali e protezione della parte debole in rapporti economici caratterizzati da evidente squilibrio trova chiaro riflesso nella legislazione europea più recente. Si pensi all'enunciato oggetto del Regolamento (UE) 2022/2065 sui servizi digitali, avente l'obiettivo di "contribuire al corretto funzionamento del mercato interno dei servizi intermediari stabilendo norme armonizzate per un ambiente online sicuro, prevedibile e affidabile che faciliti l'innovazione e in cui i diritti fondamentali sanciti dalla Carta, compreso il principio della protezione dei consumatori, siano tutelati in modo effettivo" (art. 1 Reg. ult. cit.), ciò ad esempio attraverso una disciplina delle pratiche dei fornitori di piattaforme online atte ad incidere sui processi decisionali degli utenti[37]. Ci pensi ancora, e senza pretesa di completezza, al Regolamento (UE) 2022/1925 sui mercati digitali, altresì volto ad assicurare l'equità e contendibilità dei c.d. 'controllori dell'accesso' (*gatekeepers*)[38] attraverso regole dirette a stigmatizzare pratiche sleali anche sotto il profilo del consenso al trattamento dei dati personali[39].

In questa diversa prospettiva, che dunque coniuga istanze di tutela dei diritti fondamentali e obiettivi di riequilibrio di relazioni economiche fortemente asimmetriche, a loro volta funzionali al rafforzamento del mercato interno, occorre chiedersi se il consenso al trattamento possa diventare (almeno in astratto) uno strumento di governo della circolazione dei dati e un contrappeso al potere dei titolari del trattamento. La questione presenta elementi di particolare criticità se letta alla luce del dibattito, peraltro comune al contesto consumeristico, sui limiti del consenso sotto il profilo dell'effettiva propensione dell'interessato a esercitare questo strumento di *voice* o, al contrario, a sviluppare una supina attitudine a un consenso autorizzatorio privo di qualsiasi reale funzione di governo[40].

Trascurando queste ultime sollecitazioni, secondo approcci peraltro comparabili alla regolazione consumeristica, il legislatore europeo rafforza il ruolo del consenso mediante un

---

[37] Può essere letto nella duplice prospettiva della decisione di consumo e del consenso dell'interessato l'art. 25, Reg. (UE) 2022/2065; ad esso si riferisce il Considerando 67, Reg. ult. cit., in tema di percorsi oscuri (o *dark patterns*): "I percorsi oscuri sulle interfacce online delle piattaforme online sono pratiche che distorcono o compromettono in misura rilevante, intenzionalmente o di fatto, la capacità dei destinatari del servizio di compiere scelte o decisioni autonome e informate. Tali pratiche possono essere utilizzate per convincere i destinatari del servizio ad adottare comportamenti indesiderati o decisioni indesiderate che abbiano conseguenze negative per loro. Ai fornitori di piattaforme online dovrebbe pertanto essere vietato ingannare o esortare i destinatari del servizio e distorcere o limitare l'autonomia, il processo decisionale o la scelta dei destinatari del servizio attraverso la struttura, la progettazione o le funzionalità di un'interfaccia online o di una parte della stessa. Ciò dovrebbe comprendere, a titolo non esaustivo, le scelte di progettazione a carattere di sfruttamento volte a indirizzare il destinatario verso azioni che apportano benefici al fornitore di piattaforme online, ma che possono non essere nell'interesse dei destinatari, presentando le scelte in maniera non neutrale, ad esempio attribuendo maggiore rilevanza a talune scelte attraverso componenti visive, auditive o di altro tipo nel chiedere al destinatario del servizio di prendere una decisione".

[38] Si tratta di imprese che forniscono servizi di piattaforme di base, quali punti di accesso attraverso i quali gli utenti commerciali raggiungono gli utenti finali (v. art. 3, Reg. (UE) 2022/1925).

[39] Es. art. 5, § 2, Reg. 2022/1925/UE: "Se l'utente finale ha negato o revocato il consenso prestato ai fini del primo comma, il *gatekeeper* non ripete la sua richiesta di consenso per la stessa finalità più di una volta nell'arco di un anno".

[40] B.W. SCHERMER, B. CUSTERS e S. VAN DER HOF, *The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection*, in *Ethics and Information Technology*, 2014, 171-182. DOI:10.1007/s10676-014-9343-8. V. anche I.A. CAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *Oss. dir. civ. comm.*, 2018, 67.

solido apparato di obblighi informativi, volti a garantire la piena consapevolezza dell'interessato consenziente e a ridurre, almeno in parte, l'asimmetria di potere nei rapporti con il titolare[41]. Non sfugge peraltro, come già segnalato sopra, che, ben oltre il paradigma della tutela consumeristica, tale informazione è declinata, nella prospettiva della Corte di giustizia, secondo un principio di effettività (della tutela e del volere dell'interessato), per cui l'informazione deve essere non solo data al soggetto 'debole' e non solo ricevuta da costui ma addirittura "assimilata", così da incidere non solo in astratto ma in concreto sul processo decisionale dell'interessato[42]. In questa evoluzione può ritrovarsi il tentativo di contaminare gli schemi tradizionali della tutela consumeristica con le istanze sottese alla tutela dei diritti fondamentali. Resta invece senza risposta la questione sull'effettiva idoneità dei meccanismi volti a stimolare un consenso attivo a superare i limiti indotti da un eccesso di informazione e di consultazione dell'interessato messi in luce dalle scienze comportamentali[43].

Una contaminazione ancor più problematica, tra istanze di tutela dei diritti fondamentali e obiettivi di correzione delle asimmetrie di potere nel mercato interno, pare emergere là dove si mette in dubbio il ruolo del consenso nel contesto di rapporti caratterizzati da 'evidente squilibrio' tra titolare e interessato. Secondo il Considerando 43 del Regolamento, "[p]er assicurare la libertà di prestare il consenso, è opportuno che il consenso non costituisca un valido fondamento giuridico per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato prestato liberamente in tutte le circostanze di tale situazione specifica". Non deve sfuggire che tale valutazione di opportunità, pur rilevante ai fini dell'interpretazione del GDPR, non è stata incorporata nell'art. 7 in tema di consenso (diversamente dal prosieguo del considerando, invece riflesso nel comma 4 del medesimo articolo). Al tempo stesso, anche solo sul piano interpretativo, tale riferimento apre una chiara breccia nel sistema, apparentemente allontanando le sorti dell'autodeterminazione dell'interessato (incompatibile con un assetto asimmetrico) da quelle della decisione consumeristica (compatibile con la natura asimmetrica della relazione commerciale). È dunque il consenso dell'interessato strutturalmente inidoneo a governare la circolazione dei dati nel contesto di rapporti caratterizzati da 'evidente squilibrio'?

---

[41] Comitato Europeo per la Protezione dei Dati, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, 4.5.2020, 16.

[42] Corte giust. UE, 11.11.2020, *Orange v. Romania*, cit., par. 46.

[43] Cfr. N. RICHARDS e W. HARTZOG, *The Pathologies of Digital Consent*, in *Wash. U. L. Rev.*, 2019, 1461, dove si osserva che il consenso può divenire un utile strumento di controllo nel contesto digitale attuale se la sua richiesta o espressione è infrequente, se gli effetti negativi di una cattiva scelta sono evidenti, se l'interessato ha chiari incentivi a compiere una scelta seria e consapevole.

In questa prospettiva può far riflettere che, anche nella legislazione europea più recente, ferma restando la necessità di salvaguardare la liceità del trattamento dei dati personali e dunque l'esistenza di una valida base giuridica al trattamento, sembra farsi strada un approccio volto a modulare i meccanismi di protezione in funzione dell'impatto che l'attività degli operatori possa determinare sui diritti fondamentali. Un ruolo molto rilevante è svolto, sotto questo profilo, dagli strumenti di valutazione dei rischi che gli operatori sono tenuti a predisporre tenendo conto, tra altri aspetti, degli "eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali, in particolare i diritti fondamentali alla dignità umana sancito nell'articolo 1 della Carta, al rispetto della vita privata e familiare sancito nell'art. 7 della Carta, alla tutela dei dati personali sancito nell'articolo 8 della Carta, alla libertà di espressione e di informazione, inclusi la libertà e il pluralismo dei media, sanciti nell'articolo 11 della Carta, e alla non discriminazione sancito nell'articolo 21 della Carta, al rispetto dei diritti del minore sancito nell'art. 24 della Carta, così come all'elevata tutela dei consumatori, sancito nell'articolo 38 della Carta" (così art. 34, Regolamento (UE) 2022/2065 del 19.10.2022, relativo a un mercato unico dei servizi digitali). Tale obbligo supplementare si applica soltanto ai fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi per la gestione dei rischi sistemici, a complemento di una legislazione, quale quella contenuta nel GDPR, che si applica trasversalmente ai titolari del trattamento a prescindere dalla loro dimensione e dall'impatto che la loro attività determini sui diritti fondamentali, salvo per possibili adattamenti per lo più demandati alla legislazione nazionale e alla regolazione privata (v. Considerando 13 e art. 40 GDPR).

Il riferimento all'autorità pubblica, contenuto nel Considerando 43, è sufficientemente pregnante per suggerire una pari preoccupazione nei confronti delle 'autorità private' che, proprio nel contesto dell'economia digitale, presidiano relazioni caratterizzate da 'evidente squilibrio'?
Del tema si è occupata di recente la Corte di giustizia nel caso *Meta*, già richiamato[44].
Allineandosi alle conclusioni esposte dall'Avvocato Generale, la Corte ha in parte ricomposto l'apparente frattura tra autodeterminazione informativa e decisione consumeristica sopra prospettata. Nel caso in questione, il giudice europeo ha infatti escluso che il Considerando 43 sopra richiamato debba essere interpretato nel senso di tracciare un'irriducibile incompatibilità tra consenso libero ed evidente squilibrio nella relazione tra titolare e interessato. A tal fine, con una formula che richiama l'impostazione del medesimo Considerando in tema di consenso condizionante, ha individuato nell'evidente squilibrio (la posizione dominante nel caso di specie) un importante elemento di valutazione della libertà del consenso: importante ma non esclusivo, né dirimente. Nella prospettiva della Corte, così come per i rapporti di consumo, si preserva dunque uno spazio di autodeterminazione informativa dell'interessato anche nel contesto di rapporti fortemente asimmetrici, purché sussistano altre e più pregnanti garanzie di libertà del consenso. In tal senso, sono richiamati i parametri già previsti dal Regolamento, con particolare riguardo alla specificità del consenso rispetto al singolo trattamento e alla disponibilità, per l'interessato, di "alternative equivalenti" non accompagnate dal trattamento dei dati, "se del caso a fronte di un adeguato corrispettivo"[45] e con possibilità di revoca del consenso senza pregiudizi[46].
L'asimmetria delle relazioni digitali, così come quella delle relazioni commerciali, è dunque fattore rilevante per la determinazione degli strumenti di tutela dell'interessato a garanzia dei suoi diritti fondamentali. Tuttavia, come nel diritto europeo dei rapporti diseguali, non è l'allocazione del potere economico, da sola, a indurre la reazione dell'ordinamento, né ad erigere barriere preventive all'esercizio della propria autonomia, bensì l'abuso di quel potere realizzato attraverso pratiche idonee a ostacolare la libera scelta della parte debole. Poiché, nel contesto della protezione dei dati, tale libera scelta è altresì esercizio di un diritto fondamentale, la pratica è valutata con maggior rigore (ad esempio, richiedendosi una partecipazione attiva della parte debole, normalmente non attesa dal consumatore) e all'operatore si impone un modello economico che sia compatibile con l'esercizio di un consenso ispirato al principio di effettività. Sotto questo profilo, non è un caso che il tema delle 'alternative equivalenti' al servizio abbinato al trattamento di dati personali non necessari all'esecuzione del contratto torni a catturare l'attenzione del legislatore europeo nel Regolamento sui mercati digitali in tema di pratiche sleali dei *gatekeepers*[47].

---

[44] V note 9 e 23 ss. e testo corrispondente.
[45] Sul punto v. sopra, nota 34 e testo corrispondente.
[46] Corte giust. UE, *Meta Platforms*, C-252/21, cit., par. 144-150. Deve allora intendersi che, secondo la Corte, tali 'pregiudizi' non potranno coincidere con l'eventuale 'adeguato corrispettivo', configurato dalla Corte come compatibile con la sussistenza di 'alternative equivalenti'.
[47] Regolamento (UE) 2022/1925 del 14.9.2022 relativo a mercati equi e contendibili nel settore digitale (regolamento sui mercati digitali), Considerando 36 e 37: "Per non compromettere in modo sleale la contendibilità dei servizi di piattaforma di base, i *gatekeeper* dovrebbero consentire agli utenti finali di scegliere liberamente di seguire tali pratiche di trattamento dei dati e accesso con registrazione offrendo un'alternativa meno personalizzata ma equivalente, e senza subordinare l'utilizzo del servizio di piattaforma di base o di talune sue funzionalità al consenso dell'utente finale. Ciò non dovrebbe pregiudicare la possibilità per il *gatekeeper* di procedere al trattamento dei dati personali o di fare accedere con registrazione gli utenti finali a un servizio, avvalendosi della base giuridica di cui all'articolo 6, paragrafo 1, lettere c), d) ed e), del regolamento (UE) 2016/679, ma non di cui all'articolo 6, paragrafo 1, lettere b) ed f), del medesimo regolamento. (37) L'alternativa meno personalizzata non dovrebbe essere differente o di qualità inferiore rispetto al servizio fornito agli utenti finali che prestano il proprio consenso, a meno che il deterioramento della qualità non sia una conseguenza diretta del fatto che il *gatekeeper*

Il riferimento all'effettività del consenso non vale solo a configurare le già citate 'alternative equivalenti' prive del trattamento dei dati liberamente rifiutabile, ma anche a garantire un sostanziale spazio per la sua stessa revoca, complemento necessario del diritto fondamentale all'autodeterminazione informativa. Del tema si è occupata di recente la Corte di giustizia nel caso *Proximus*, quale operatore di servizi di consultazione di elenchi telefonici accessibili al pubblico, costruiti in collaborazione tra più operatori attraverso una condivisione di dati trasmessi dai clienti che abbiano acconsentito alla pubblicazione. In un simile contesto, il rapporto asimmetrico tra singolo interessato e singolo titolare è reso ulteriormente complesso dalla circolazione dei dati tra i diversi operatori. La presenza di più titolari, per quanto comunicata all'interessato consenziente, accresce l'asimmetria di potere nei rapporti tra titolare e interessato e si trasforma in un ostacolo all'effettività dell'autodeterminazione informativa, da esercitarsi presso ciascuno dei titolari. Facendo applicazione del principio di effettività, la Corte di giustizia ha temperato questa asimmetria riconoscendo, in capo al fornitore destinatario dell'istanza di revoca, un preciso obbligo di trasmettere la medesima richiesta ai diversi fornitori e ai motori di ricerca[48]. Perché il consenso e la sua revoca siano strumenti di governo della circolazione dei dati personali nel contesto di rapporti asimmetrici, sul titolare grava un onere organizzativo volto a contenere, almeno in parte, gli effetti quella asimmetria.
Se dunque, per un verso, la giurisprudenza europea continua a vedere nel consenso dell'interessato un importante pilastro della tutela dei diritti fondamentali incisi dalla circolazione dei dati, per l'altro verso, può osservarsi, tanto nella legislazione, quanto nella giurisprudenza europea, una crescente rilevanza di strumenti complementari di tutela, volti a contrastare pratiche scorrette nel contesto di rapporti economici di tipo asimmetrico e dunque a garantire il buon funzionamento del mercato prima ancora di o comunque insieme alla tutela dei diritti fondamentali.
Si tratta di un approccio che, lungi dal depotenziare il tratto distintivo del modello europeo fondato sulla tutela dei diritti fondamentali, tende a rafforzarlo facendo leva su una complementarità di tutele del tutto coerente con il principio di effettività[49]. Del resto, se è vero che gli strumenti volti a correggere le asimmetrie di potere tendono a garantire talune condizioni di esercizio della libertà da parte dell'interessato, senza reali garanzie che il singolo individuo abbia in concreto letto, compreso (assimilato?) e dunque deciso in modo consapevole, è altresì dimostrato che una ricerca granulare e sistematica del consenso informato, quale esercizio della fondamentale e libera autodeterminazione, non conduca a risultati concretamente apprezzabili in termini di partecipazione degli individui al governo dei dati[50]. Ne è, in un certo senso, prova la recente ricerca del legislatore di favorire forme di supporto all'esercizio dei diritti fondate sulla delega ad organizzazioni collettive, investite non del mero compito di amministrare diritti economici connessi al godimento di diritti fondamentali ma alla stessa prestazione del consenso quale cuore pulsante di un'autodeterminazione informativa[51].

---

non possa procedere al trattamento dei dati personali o fare accedere con registrazione gli utenti finali a un servizio.".

[48] Ciò in forza dell'art. 19, che prevede un simile obbligo in ipotesi di richiesta di cancellazione del dato, salvo che ciò implichi uno sforzo sproporzionato. V. Corte giust. UE, 27.10.2022, *Proximus NV*, C-129/21, ECLI:EU:C:2022:833, par. 82 e 85.

[49] F. CAFAGGI, *Judicial and Administrative Protection Intertwined. The Right to an Effective, Proportionate and Dissuasive Remedy*, in *Civil Courts and the European Polity. The Constitutional Role of Private Law Adjudication in Europe*, a cura di C. Mak e B. Kas, Bloomsbury, Londra, 2023, 175.

[50] N. RICHARDS e W. HARTZOG, *The Pathologies of Digital Consent*, cit., part. 1476 ss.; B.W. SCHERMER, B. CUSTERS e S. VAN DER HOF, *The Crisis of Consent*, cit.

[51] V. (UE) 2022/868, 30.5.2022, relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla *governance* dei dati), Considerando 31: "Le cooperative di dati mirano a raggiungere una serie di obiettivi, in particolare a rafforzare la posizione dei singoli individui, affinché compiano

Accettata la complementarità tra diversi approcci regolatori, si tratta di capire quali siano le pratiche professionali dei grandi operatori volte a garantire un'effettiva partecipazione dell'individuo al governo dei dati, anche attraverso la prestazione del consenso al trattamento dei dati personali. Sotto questo profilo paiono molto utili le letture comportamentaliste che inducono a preferire una informazione più selettiva e focalizzata sui profili determinanti e una ricerca non ossessiva del consenso, inteso non come forma di autorizzazione e avallo di trattamenti unilateralmente determinati, ma come partecipazione effettiva e realmente consapevole[52]. Sul piano della regolazione, questo approccio, solo in parte emergente nelle iniziative più recenti, porterebbe a calibrare obblighi informativi e coinvolgimento dell'interessato in funzione del rischio di impatto sui diritti fondamentali dell'individuo, della natura del dato trattato (es. se appartenente a speciali categorie *ex* art. 9 GDPR), della finalità del trattamento e dell'eventualità di usi secondari, dell'effettiva esistenza di uno spazio di revoca e (o) di retrocessione del trattamento. Una applicazione del diritto vigente rispettosa dei principi di effettività e proporzionalità potrebbe portare ad approdi più efficaci nella stessa prospettiva di un'elevata tutela dei diritti fondamentali[53].

4. Complementarità degli approcci e tutela effettiva dei diritti fondamentali.

Muovendo dalle considerazioni appena esposte, il tema regolatorio si interseca con le questioni inerenti alla tutela effettiva del diritto alla protezione dei dati personali. È chiaro infatti che tanto maggiore è la difficoltà di ripristinare *ex post* le condizioni di legittimità del trattamento ed eliminare le conseguenze del trattamento illecito, tanto più rilevante è assicurare *ex ante* un efficace controllo sulle condizioni di legittimità e, se applicabile, un adeguato spazio per l'espressione di un consenso consapevole. Viceversa, là dove gli strumenti di controllo *ex ante*, inclusa la manifestazione di un consenso pieno e non meramente autorizzatorio, siano strutturalmente deboli, perché ad esempio l'uso di determinate tecnologie o di talune pratiche degli operatori inducono l'interessato a sottovalutare o non considerare i rischi derivanti dal trattamento dei dati, allora assume particolare rilevanza la ricerca di rimedi effettivi operanti a posteriori contro il trattamento privo di adeguata base giuridica[54].
A tal fine è importante aver riguardo non solo agli strumenti messi a disposizione delle autorità di controllo e di quelle giudiziarie dai regolamenti europei in tema di protezione dei dati personali, tanto sotto il profilo delle misure preventive che di quelle correttive e risarcitorie, ma anche e sempre più dell'ampia gamma dei rimedi consumeristici, in taluni casi estesi

scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del gruppo, o trovando possibili soluzioni alle posizioni contrastanti dei singoli membri di un gruppo in merito alle modalità di utilizzo dei dati laddove tali dati riguardino più interessati all'interno di tale gruppo. In tale contesto è importante riconoscere che i diritti a norma del regolamento (UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunciarvi. Le cooperative di dati potrebbero altresì rappresentare uno strumento utile per imprese individuali e PMI che, in termini di conoscenze in materia di condivisione dei dati, sono spesso equiparabili ai singoli individui".

[52] N. RICHARDS e W. HARTZOG, *The Pathologies of Digital Consent,* cit.

[53] Si tratta di una prospettiva di ricerca sviluppata nell'ambito del progetto europeo di formazione giudiziaria FRICoRe, i cui risultati sono in parte confluiti nei *Casebook* sulla tutela effettiva dei diritti fondamentali in diverse aree del diritto europeo (disponibili alla pagina https://www.fricore.eu/content/materials), in parte nei contributi contenuti nel volume a cura di P. IAMICELI, *Effettività delle tutele e diritto europeo. Un percorso di ricerca per e con la formazione giudiziaria,* Napoli, 2020.

[54] Sul rapporto tra tutele *ex ante* ed *ex post,* F. CAFAGGI, *Judicial and Administrative Protection Intertwined*, cit., e, per ulteriori sviluppi dell'analisi, F. CAFAGGI e P. IAMICELI, *The right to an effective remedy and its constitutional foundations*, di prossima uscita.

espressamente a tutela dell'interessato, quale parte debole del rapporto[55]. Il ruolo del giudice europeo è stato, anche sotto questo profilo, assai rilevante e ha da tempo chiarito la complementarità tra i due ambiti della tutela, così suggellando, anche in termini rimediali, la natura composita della regolazione sulla circolazione dei dati a cavallo tra tutela dei diritti fondamentali e buon funzionamento del mercato[56].
Peraltro, è utile sottolineare come, in prospettiva di bilanciamento e in applicazione del principio di proporzionalità, la tutela effettiva dell'interessato non passi necessariamente attraverso il completo sbarramento alla circolazione del dato personale. La sospensione del trattamento, la ricerca di tecniche di minimizzazione dello stesso, la deindicizzazione come alternativa alla cancellazione del dato, i progressi sul versante dell'anonimizzazione o pseudo-anonimizzazione dei dati sono esempi di approcci rimediali che talora la stessa giurisprudenza europea ha sollecitato nel tentativo di ristabilire un giusto equilibrio degli interessi in gioco[57].
Un simile bilanciamento può diventare ancora più pregnante quando si combinano istanze di tutela dei diritti fondamentali e di riequilibrio delle relazioni asimmetriche volte alla correzione di pratiche scorrette e al miglior funzionamento del mercato. Viene allora in primo piano l'esigenza di salvaguardare l'accesso della parte debole al bene o servizio, contenendo gli effetti del rimedio in modo da non travolgere l'intera operazione economica o la partecipazione dell'interessato alla rete sociale di elezione[58]: un approccio ben noto al diritto europeo del consumo e della nullità parziale in ipotesi di clausole abusive e in tal senso estendibile agli effetti del consenso invalido quando collegato alla stipulazione di contratti per l'acquisto di beni e servizi[59]. Come nel contesto consumeristico, il rimedio configura una protezione

[55] V. Direttiva (UE) 2020/1828 relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori, il cui ambito di applicazione si estende alla tutela dei consumatori anche a fronte di violazioni della legislazione in tema di protezione dei dati personali. Sulla complementarità tra tutela consumeristica e tutela dei dati personali, v. in giurisprudenza, Corte giust. UE, 28.4.2022, *Meta Platforms Ireland Limited*, già *Facebook Ireland Limited*, C-319/20, ECLI:EU:C:2022:322, par. 74-76.

[56] Sul tema, per un'ampia analisi relativa al dialogo tra corti europee e nazionali, sia consentito il rinvio a P. IAMICELI, F. CAFAGGI e A. ANGIOLINI (a cura di), *Casebook Effective Data Protection and Fundamental Rights*, Roma, 2022, disponibile su https://www.fricore.eu/content/materials, e, già precedentemente, F. CASAROSA, *Azioni collettive fra tutela dei dati personali e tutela dei consumatori: nuovi strumenti alla prova dei fatti*, in *Effettività delle tutele e diritto europeo*, cit.

[57] A partire dal noto caso deciso dalla Corte giust. UE, 13.5.2014, *Google Spain SL*, C-131/12, ECLI:EU:C:2014:317, sulla deindicizzazione, rimedio su cui la Corte di giustizia è tornata più volte per definirne i confini nella prospettiva del bilanciamento richiamata nel testo (cfr., tra le ultime, Corte giust. UE, 24.9.2019, *GC et Al*, C-136/17, ECLI:EU:C:2019:773; Corte giust. UE, 8.12.2022, *Google LLC*, C-460/20, ECLI:EU:C:2022:962).

[58] Per ipotesi, la caducazione dell'intero contratto potrebbe essere argomentata ove si riconoscesse rilevanza causale alla prestazione del consenso secondo lo schema dello scambio 'bene o servizio verso dati' (sul tema v. G. RESTA, *I dati personali oggetto del contratto*, cit., 148, con riferimento alla situazione in cui si dimostri che la possibilità di procedere a un lecito trattamento dei dati personali costituisca, nell'economia del rapporto, una vera e propria 'base negoziale'). Diversamente, ove la funzione remuneratoria fosse solo parziale e comunque non essenziale nell'assetto di interessi delle parti, si porrebbe il diverso problema della possibile rideterminazione dell'equilibrio contrattuale, su cui v. oltre nel testo.

[59] Con riferimento alle clausole vessatorie, il tema è ampiamente discusso nel contesto dei mutui indicizzati, là dove, pur in presenza di una vessatorietà incidente su elementi essenziali del sinallagma negoziale, la giurisprudenza ha sviluppato tecniche interpretative volte a salvaguardare l'interesse del consumatore alla continuità contrattuale, circoscrivendo, per quanto possibile, gli effetti della violazione alla sola clausola vessatoria; v., *ex multis*, Corte giust. UE, 3.3.2020, *Gómez*, C-125/18, par. 67, ECLI:EU:C:2020:138. Trasposto questo approccio, fondato sul principio di effettività della tutela, nel contesto di contratti aventi ad oggetto la fornitura di servizi o contenuti digitali, che prevedano il trattamento di dati personali, la cui base giuridica sia assente (in quanto ad esempio fondata su un consenso invalido), il principio di effettività porterebbe a prediligere i rimedi ripristinatori rispetto a quelli caducatori al fine di salvaguardare l'accesso del consumatore al servizio e dunque la continuità contrattuale.

unilaterale al precipuo fine di correggere lo squilibrio esistente nella relazione. Su questa scia, e ancora in forza del principio di effettività della tutela, dovrebbe ammettersi la rilevabilità d'ufficio della violazione del dato personale, largamente riconosciuta a tutela dei consumatori[60].

Parimenti, potrebbe assumere rilievo il ricorso alla c.d. nullità punitiva, di matrice consumeristica, là dove il consenso (invalido) dell'interessato sia stato acquisito con finalità remuneratorie. In tal caso, l'applicazione consumeristica dei principi generali di effettività, proporzionalità e dissuasività (comunque rilevanti nel contesto della protezione dei dati personali) potrebbe portare ad escludere, per un verso, la caducazione dell'intero contratto, come evidenziato poco sopra, e, per l'altro (e qui l'effetto punitivo e dissuasivo), l'integrazione del contratto sotto il profilo della ri-determinazione del prezzo[61]. Secondo questa prospettiva, non ancora esplorata nella giurisprudenza esistente, venuta meno la base consensualistica del trattamento e dunque la stessa remunerazione (o remunerazione concorrente) del servizio, al titolare verrebbe preclusa l'applicazione di clausole contrattuali che, in assenza di consenso al trattamento di dati non necessari all'esecuzione del contratto, prevedano un prezzo o un maggior prezzo per il bene o servizio acquistato[62]. Il contratto di fornitura di beni o servizi, con cui si sia estorto un consenso invalido al trattamento di dati personali, resterebbe perciò gratuito o beneficerebbe dello sconto previsto, anche là dove si facesse valere la nullità del consenso al trattamento dei dati, a cui originariamente era condizionata la gratuità ovvero lo sconto.

5. Alcuni rilievi conclusivi

L'uso ormai inarrestabile delle tecnologie digitali e la crescita esponenziale di mercati largamente dipendenti dalla circolazione di dati, personali e non, mettono a dura prova il paradigma del consenso quale cardine della tutela del diritto fondamentale all'autodeterminazione informativa, esaltandone piuttosto una sterile funzione autorizzatoria a supporto di logiche di mera *compliance* dal lato dell'operatore. Un approdo, quest'ultimo, che contraddice le intenzioni, animate piuttosto dall'esigenza di garantire un elevato livello di protezione del diritto fondamentale sotteso all'esercizio del consenso, esigenza che ha portato, tanto nella legislazione, quanto nella giurisprudenza, a separare le sorti del consenso da quelle del contratto di consumo, valorizzando il ruolo dell'informazione e dell'autodeterminazione dell'interessato, quali strumenti della *voice* dell'individuo a protezione di interessi non riducibili a 'merci' e, come tali, non alienabili. Probabilmente quell'esigenza può essere perseguita per altre vie.

Gli sviluppi più recenti restituiscono infatti un quadro assai più poliedrico e meno polarizzato, in cui la circolazione dei dati è sempre meno sacrificabile in nome di una maggior tutela dei

---

Sulla configurazione della violazione dei diritti dell'interessato alla stregua di una non conformità di servizi o contenuti digitali ai sensi della Direttiva 2019/770/UE, C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770*, cit.).

[60] P. IAMICELI, F. CAFAGGI e A. ANGIOLINI (a cura di), *Casebook Effective Data Protection and Fundamental Rights*, cit., 8.

[61] V., in materia consumeristica, Corte giust. UE, 14.6.2012, Case C-618/10, *Banco Español de Crédito*, EU:C:2012:349; Corte giust. UE, 30.5.2013, Case C-488/11, *Asbeek Brusse*, EU:C:2013:341; Corte giust. UE, 3.10.2019, Case C-260/18, *Dziubak*, EU:C:2019:819; Corte giust. UE, 14.3.2019, Case C-118/17, *Dunai*, EU:C:2019:207.

[62] Sul tema delle nullità punitive in ambito consumeristico, sia consentito il rinvio a P. IAMICELI, *Nullità parziale e integrazione del contratto: riflessioni sul diritto del consumatore a un rimedio effettivo, proporzionato e dissuasivo*, in *Liber Amicorum per Giuseppe Vettori*, a cura di G. Passagnoli, F. Addis, G. Capaldo, A. Rizzi e S. Orlando, Firenze, 2022, 1687 ss.; e, più recentemente, ID., *The 'Punitive Nullity' of Unfair Terms in Consumer Contracts and the Role of National Courts: a Principle-Based Analysis*, in *EuCML*, 2023, 4, 142 ss.

diritti fondamentali, e sempre più necessaria nel perseguimento di politiche di sviluppo tecnologico, economico, sociale, ambientale, geopolitico. Nuovi equilibri si rendono necessari e, rispetto alla relazione discreta tra singolo titolare e singolo interessato, maggior rilievo assume l'assetto complessivo dei poteri in gioco e la presenza di squilibri e asimmetrie strutturali[63].

In questo mutato contesto, in cui non a caso guadagnano spazio la regolazione pubblicistica e le forme di tutela amministrativa, il consenso dell'interessato si attesta sempre più come strumento, se non di governo della circolazione dei dati, almeno di parziale contrappeso allo strapotere dei titolari. Perché questa funzione possa essere assolta e affinché possa garantire un elevato livello di protezione dei sottesi diritti fondamentali, gli strumenti di regolazione e le forme di tutela non potranno che muovere dalla constatazione di questi squilibri e dunque far tesoro della ricca esperienza maturata dal diritto europeo, con particolare riguardo a quello di matrice giurisprudenziale, nel campo dei rapporti asimmetrici, a partire dall'area consumeristica. Lungi dal depotenziare la tutela dei diritti fondamentali, tale contaminazione è volta a rafforzare quella tutela in modo del tutto coerente con l'applicazione dei principi di effettività, proporzionalità e dissuasività delle tutele, largamente applicati dalla Corte di giustizia ben oltre la materia del diritto dei consumatori[64]. Nella precipua prospettiva dei diritti fondamentali, la natura degli interessi coinvolti sarà peraltro ancora rilevante per declinare le diverse matrici impiegate dai giudici nazionali nell'individuazione del rimedio effettivo, proporzionato e dissuasivo. Le corti infatti non potranno prescindere da un bilanciamento tra i diversi interessi in gioco, né dalla consapevolezza dei limiti comportamentali indotti tanto dall'eccesso di informazione quanto dalle richieste compulsive di consensi autorizzatori: limiti comportamentali che assumono caratteristiche profondamente diverse quando la scelta della parte debole ha a che fare con interessi esclusivamente economici o con l'esercizio di diritti fondamentali[65].

In una fase del diritto europeo in cui molto è stato prodotto sul versante della regolazione, tanto è ancora da attendersi da parte della giurisprudenza, che è da tempo impegnata in un dialogo costruttivo tra corti europee e corti nazionali nel quadro di principi generali[66]. Quali elementi portanti di una cultura giuridica europea costruita, anche grazie ai giudici, sulle tradizioni costituzionali comuni, sui diritti e le libertà fondamentali, saranno questi principi a orientare i nuovi approdi del dialogo tra le corti aperto a una maggiore integrazione tra aree diverse del diritto europeo dei rapporti di mercato diseguali.

---

[63] Tali equilibri sono al centro della più recente legislazione europea, con particolare riferimento al Regolamento 2022/1925/UE (regolamento mercati digitali), cit.

[64] F. CAFAGGI e P. IAMICELI, *The Principles of Effectiveness, Proportionality and Dissuasiveness in the Enforcement of EU Consumer Law: The Impact of a Triad on the Choice of Civil Remedies and Administrative Sanctions*, in *European Review of Private Law*, 2017, 575–618; C. PAVILLON, *Private Enforcement as a Deterrence Tool: A Blind Spot in the Omnibus-Directive*, in *European Review of Private Law*, 2019, 1297. Di prossima uscita, F. CAFAGGI e P. IAMICELI, *The right to an effective remedy and its constitutional foundations*, cit.

[65] Si pensi alla capacità della parte debole di elaborare una certa informazione al fine di valutare il rischio sotteso a una certa scelta (es., acconsentire o meno al trattamento di dati sanitari, ovvero accettare o meno un certo schema di computo degli interessi del mutuo), posto che l'avversità al rischio può essere molto diversa a seconda che si abbia a che fare con il rischio di perdite economiche o con il rischio di subire decisioni discriminatorie o comunque lesive della propria personalità. Sulla possibilità di modulare la regolazione del consenso in base all'effettivo impatto sui diritti dell'interessato, v. N. RICHARDS e W. HARTZOG, *The Pathologies of Digital Consent*, cit.

[66] G. VETTORI, *Effettività tra legge e diritto*, cit., 105 ss.

AUTORI

Gabriele Carapezza Figlia – *Professore ordinario presso l'Università di Roma, LUMSA*

Ginevra Cerrina Feroni – *Vice Presidente dell'Autorità Garante per la protezione dei dati personali*

Giusella Finocchiaro – *Professore ordinario presso l'Università di Bologna*

Paola Iamiceli – *Professore ordinario presso l'Università di Trento*

Salvatore Orlando – *Professore ordinario presso l'Università di Roma, La Sapienza*

Vincenzo Ricciuto – *Professore ordinario presso l'Università di Roma, Tor Vergata*

Pasquale Stanzione – *Presidente dell'Autorità Garante per la protezione dei dati personali*

Giuseppe Vettori – *Professore ordinario presso l'Università di Firenze*