GIURETA
Rivista di Diritto dell'Economia, dei Trasporti e dell'Ambiente
Vol. XIX
2021

CONSENSO DELL'INTERESSATO E DATI PERSONALI AL TEMPO DEI *BIG DATA*

Francesco Stassi[*]

SOMMARIO: 1. Premessa – 2. Consenso, regolazione normativa e tutela del dato personale – 2.1. Il ruolo del consenso dell'interessato nel GDPR: verso una lettura negoziale? – 2.2. La perdita di centralità del consenso del titolare – 2.3. L'apporto della direttiva 2019/770/UE – 2.4. Il consenso "granulare" – 3. Consenso e *big data*. – 4. Conclusioni.

1. – L'incremento esponenziale di dati personali in circolazione nella cornice di un'economia prevalentemente digitalizzata sollecita una costante verifica dell'adeguatezza del modello di disciplina a contemperare equamente le istanze di tutela della persona e della protezione del dato con quelle di utilizzo di quel dato ad opera dei principali operatori del mercato come fattore di competitività. Dinanzi alla necessità delle organizzazioni complesse di avvalersi di pratiche commerciali personalizzate, che incarnino le logiche della *mass customization* - e dunque dinanzi alla loro attitudine allo sfruttamento di una vasta mole di dati analitici (i c.d. *big data analytics*), funzionali alla previsione delle scelte dell'utente, e segnatamente quelle di consumo - si assiste a un fenomeno di progressiva riqualificazione del consenso: a un modello incentrato sull'autodeterminazione individuale segue il suo abbandono, mosso dalla presa d'atto che il dato personale circola e sarà utilizzato anche in forma aggregata per strategie di mercato. La profilazione dei dati consente infatti di classificare gli utenti in gruppi, che manifestano preferenze omogenee in base a gusti, a interessi e a comportamenti. In un siffatto contesto, dell'enfasi rivolta al consenso nell'ottica della protezione del dato personale sembra essersi persa traccia[1], dinanzi all'emersione di un consenso che si palesa o strumentale all'accesso di un servi-

[*] Cultore in Diritto privato presso l'Università degli studi di Palermo.

[1] Così C. Basunti, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contr. Impr.*, 2/2020, 860 ss.

ISSN 1724-7322

zio dell'utente o rarefatto a causa del *trend* di de-personalizzazione del dato acquisito da strategie di studio su ampia scala[2].

La presente trattazione si propone quindi di indagare il ruolo del consenso manifestato dall'utente all'utilizzo del dato personale alla luce del connubio generato da: *a*) dall'attuale regolazione, che trova nel regolamento 2016/679/UE, "*General Data Protection*" (di seguito, *GDPR*), il principale referente normativo; *b*) dalla crescente propensione alla patrimonializzazione del dato personale, che si concilierebbe con una lettura negoziale della natura giuridica del consenso; *c*) dalla positivizzazione dello schema di cessione del dato personale ad opera della direttiva 2019/770/UE, che sollecita una "consumerizzazione" della protezione dei dati personali; *d*) e, infine, dall'espansione della capacità informativa dell'utente e dalla conseguente difficoltà di sorreggerne il suo utilizzo con la signoria del consenso.

L'analisi prospettata tuttavia sfugge a una ricostruzione sistematica della natura del consenso e del ruolo che esso assume, a fronte dell'impossibilità di un inquadramento unitario della materia, animata da numerose tipologie di trattamento e di dati.

2. – Come è noto, con il *GDPR*, la disciplina del trattamento dei dati personali ha subito un profondo *restyling*, rispetto alla disciplina scaturente dalla sequenza normativa "direttiva 1995/46/CEE – legge 31 dicembre 1996, n. 675 – direttiva 2002/58/CE, c.d. *E-privacy* – decreto legislativo 30 giugno 2003, n. 196 (cod. *privacy*)" [3].

La regolazione affidata alla direttiva 1995/46/CEE – recepita in Italia con la legge 31 dicembre 1996, n. 675 – nel tentativo di armonizzare la protezione dei diritti fondamentali della persona negli Stati membri rispondeva all'esigenza di conciliare la libera circolazione dei dati nel contesto intracomunitario, conformemente alle libertà fondamentali istituite con il Trattato di Maastricht, con le potenziali lesioni dei diritti della persona, e nello specifico del rispetto alla riservatezza, quale diritto di escludere altri da informa-

[2] Cfr. A. Montalero, *La* privacy *all'epoca dei* Big data, in *I dati personali nel diritto europeo*, a cura di V. Cuffaro-R. D'Orazio-V. Ricciuto, Torino, 2019, 1182 ss.

[3] Sul consenso nel codice della privacy, tra i tanti, si veda S. Mazzamuto, *Il principio del consenso e il problema della revoca*, in *Libera circolazione e protezione dei dati personali*, a cura di R. Panetta, Milano, 2006, 993 ss.

zioni riguardanti la propria sfera giuridica [4]. Una tale prospettiva regolatoria incarnava, dunque, la logica della protezione di un diritto della personalità, quale la riservatezza, nell'alveo del quale era ricompresa la tutela da trattamenti illeciti del dato personale. In quel contesto ha origine la definizione di consenso della persona interessata, quale forma di tutela individuale della persona, che si riferisce a «*qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta i dati personali che siano oggetto di un trattamento*», pedissequamente riprodotta all'art. 4 n. 11 *GDPR* [5], nonostante il mutamento di paradigma che ne sterilizza la portata.

Nel regolamento del 2016 – rispetto al quale il cod. *privacy* è stato riadeguato per il tramite del decreto legislativo 10 agosto 2018, n. 101 – il consenso del titolare è infatti da ricalibrare in considerazione dell'enfasi che connota il momento circolatorio dei dati personali e che sbiadisce sia le implicazioni personalistiche del dato personale, sia la prevalenza assiologica del diritto della personalità rispetto a un'istanza di fruizione generale delle informazioni [6]. L'attenzione originariamente rivolta al *data subject*, al titolare del dato ossia all'interessato, nella disciplina europea più recente viene indirizzata al c.d. "titolare del trattamento", colui che determina i mezzi e le finalità del trattamento (art. 4 n. 7 *GDPR*), o sul soggetto che ne è "responsabile", colui che tratta i dati per conto del titolare (art. 4 n. 8 *GDPR*).

L'inversione di tendenza che implica che la protezione del dato non sia più una prerogativa assoluta dell'interessato è consacrata dalla tensione tra due linee direttrici, simmetriche e opposte, della disciplina di matrice europea: libertà e responsabilità.

La libertà è desumibile dallo spostamento del baricentro di quel bilanciamento tra l'interesse legittimo al trattamento e il diritto dell'interessato in

[4] Si veda, in proposito, F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, in *I dati personali nel diritto europeo*, Torino, 2016, spec. 43 ss.

[5] L'art. 4 n. 11 del regolamento europeo del 2016 definisce il consenso dell'interessato come «*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] In tal senso F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2/2017, 375, che osserva che l'intervento del legislatore europeo «*non si è limitato a restituire il diritto vigente in chiave prevalentemente ricognitiva, come nella tradizione dei* Restatement*, ma ha compiuto scelte significative di politica del diritto*».

senso indubbiamente più propizio al titolare del trattamento. Ma d'altronde all'esito di una valutazione comparativa tra le due poste in gioco si è osservato che le possibilità di incisione e di compressione soprattutto del diritto alla *privacy* consentite dal Regolamento appannano la sua natura di diritto fondamentale e inviolabile, indiscussa piuttosto nei trattati europei [7].

A riprova di ciò, il *GDPR* contempla all'art. 20 il c.d. diritto alla portabilità dei dati, grazie al quale l'interessato è legittimato a pretendere dal titolare del trattamento la messa a disposizione dei propri dati personali da questi detenuti e a ottenerli in un formato strutturato, di uso comune e leggibile da dispositivo automatico, per poterli poi trasmettere a un altro titolare senza alcun impedimento, nel caso di trattamenti fondati sul consenso o di quelli fondati sulla necessità di eseguire un contratto di cui è parte l'interessato stesso o di svolgere le relative trattative, e sempre che si tratti di operazioni svolte con mezzi automatizzati.

La seconda direttrice di disciplina, da contrappeso a una circolazione di dati personali "libera", si riscontra nel principio di *accountability* [8], che comporta una responsabilizzazione del titolare del trattamento a fronte dell'obbligo vincolante per tutti i responsabili del trattamento di attuare misure e procedure per la protezione del dato, nonché per la dimostrazione della liceità del trattamento, come desumibile dagli artt. 24 e 32 *GDPR* [9]. Sotto

[7] Così A. Iuliani, *Note minime in tema di trattamento dei dati personali*, in *Europa dir. priv.*, 2018, 306 ss.; F. Piraino, *I "diritti dell'interessato" nel Regolamento generale sulla protezione di dati personali*, in *GDPR tra novità e discontinuità*, a cura di R. Caterina, in *Giur. it.*, 12/2019, 2799.

[8] Nel parere 3/2010 reso dal Gruppo di lavoro Articolo 29 (WP29) sulla protezione dei dati personali sono individuati i due elementi, nei quali si articola l'*accountability*: la necessità che il titolare del trattamento adotti misure appropriate ed efficaci per attuare i principi di protezione dei dati; nonché la necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci. Sul principio di *accountability*, tra i più, si veda G. Finocchiaro, *Il principio di* accountability, in *GDPR tra novità e discontinuità*, a cura di R. Caterina, in *Giur. it.*, 12/2019, 2778 ss.; nonché R. Caterina, *Novità e discontinuità nel Regolamento generale sulla protezione dei dati personali*, cit., 2777, che osserva che «*è l'adozione del principio di* accountability *a rivoluzionare, al di là della continuità di molte singole disposizioni, l'impianto generale dell'intera disciplina. Alla luce di tale principio si deve leggere anche il richiamo tra le condizioni di liceità del trattamento del "legittimo interesse" del titolare, già presente nella direttiva ma peraltro largamente ridotto nella sua portata dal legislatore italiano, e che comunque pare assumere nel contesto del Regolamento una nuova centralità*».

[9] Cfr. G. Finocchiaro, *Il principio di* accountability, in *GDPR tra novità e discontinuità*, a cura di R. Caterina, cit., 2779, che riscontra un secondo livello di responsabilizzazione – in linea

questo profilo, l'art. 7 del regolamento, che prevede 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*», riserva al titolare del trattamento e della scelta della modalità di acquisizione del consenso e della conseguente dimostrazione di averlo acquisito.

La maggiore sensibilità rivolta allo sfruttamento dei dati personali, anche a scapito della protezione dell'individuo, è desumibile da una serie di indici normativi rivelatori [10], tra i quali: *a*) un giudizio di compatibilità tra la finalità originaria del trattamento e la diversa finalità, pur ammesse e lecite *ex* art. 5, par. 1, lett. *b*), *GDPR*, delle successive operazioni sui dati; *b*) l'individuazione ai sensi dell'art. 21, par. 1, *GDPR*, dei motivi di opposizione dell'interessato per motivi connessi alla sua situazione particolare dinanzi al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento o 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); *c*) la sufficienza del consenso dell'interessato per le categorie particolari di dati sensibili (come quelli inerenti alla salute), per le quali l'art. 26 cod. *privacy*, oggi abrogato, prevedeva l'autorizzazione del Garante.

2.1. – Sullo sfondo delle considerazioni fin qui svolte, una ricognizione del

con quanto previsto dal citato parere 3/2010 del Gruppo di lavoro Articolo 29 - nei sistemi di responsabilità di natura volontaria, eccedenti le norme di legge minime, in relazione ai principi fondamentali di protezione dei dati o in termini di modalità di attuazione o di garanzia dell'efficacia delle misure.

[10] Così F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, cit., 380.

ruolo del consenso dell'interessato è orientata dalle disposizioni degli artt. 6 (*liceità del trattamento*), 7 (*condizioni per il consenso*) e 8 (*condizioni per il consenso dei minori in relazione ai servizi della società dell'informazione*) del *GDPR*.

Dalla prima delle tre previsioni normative discende che il consenso al trattamento dei propri dati personali per una o più specifiche finalità è una delle condizioni di liceità del trattamento, ma la perdita di centralità della volontà dell'interessato è inequivocabilmente sottesa alla possibilità che il trattamento sia altresì lecito pur prescindendo da esso [11]. Il consenso costituisce quindi uno dei fondamenti giuridici del trattamento, che non deve essere inteso come il presupposto di legittimazione principale, perchè altri presupposti possono essere presi in considerazione altri, magari più appropriati nell'ottica sia del titolare sia dell'interessato [12].

Il consenso riveste dunque una posizione decentrata, perché nella logica del Regolamento tutte le basi giuridiche hanno un'analoga valenza [13], e il consenso dell'interessato è solo una delle condizioni possibili di liceità. Semmai, il consenso dell'interessato è una condizione di liceità correlata dal legislatore soltanto alle finalità determinate, non rendendosi necessaria una valutazione di necessità del trattamento, che è piuttosto assorbita dal manifestato assenso al trattamento. Diversamente, per tutte le altre condizioni, l'art. 6 *GDPR* condiziona la liceità del trattamento, non sorretto dal consenso dell'interessato, al requisito della necessità di quel trattamento al raggiungimento delle finalità individuate: oltre lo spettro del consenso il parametro della necessità del tratta-

[11] L'art. 6 reg. *GDPR* prevede infatti che il trattamento sia altresì lecito quando: «b) *il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;* c) *il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;* d) *il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;* e) *il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;* f) *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*».

[12] C. Basunti, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, cit., 873.

[13] D. Poletti, *Le condizioni di liceità del trattamento dei dati personali*, in *GDPR tra novità e discontinuità*, a cura di R. Caterina, cit., 2785.

mento entra dunque a comporre la stessa nozione di liceità [14]. Accertata la necessità del trattamento con esito positivo, occorre superare il test di proporzionalità della compressione del diritto alla protezione dei dati personali, che si misura nei termini della correttezza del trattamento, misura e criterio di valutazione dell'*accountability* del titolare. Quest'ultimo – come si è riferito, a norma dell'art. 24 *GDPR* – deve individuare misure tecniche e organizzative adeguate alla natura, alla finalità, al contesto, all'ambito di applicazione del trattamento.

Soffermando l'attenzione sul consenso, la trasparenza e la correttezza del trattamento dei dati sono garantite già nella fase anteriore al trattamento, allorquando viene previsto l'obbligo per il titolare del trattamento di fornire agli interessati, quale condizione di legittimità del consenso, l'informativa relativa alle finalità e alle modalità del trattamento dei dati forniti (art. 12 *GDPR*). L'informativa deve essere facilmente accessibile e intellegibile per l'interessato (conformemente al considerando 39 *GDPR*) e va resa per iscritto o con altri mezzi, come la posta elettronica, ma se richiesto dall'interessato l'informativa può essere resa anche oralmente.

Il trattamento supportato dal consenso dell'interessato è poi soggetto alle condizioni dell'art. 7 *GDPR*. Una siffatta previsione normativa, oltre a porre sul titolare del trattamento l'onere di dimostrare il consenso dell'interessato, prevede che se il consenso è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Il consenso, dunque, deve essere specifico e distinguibile, chiaro e comprensibile, altrimenti non sarebbe vincolante. Di tutta evidenza tuttavia il cambio di rotta rispetto a prevedere – come nella prima legge italiana in materia di protezione di dati personali – una regola del consenso "espresso". Nella disciplina del regolamento europeo il presupposto di validità del consenso, oltretutto, è la sua libera prestazione da parte dell'interessato, per il cui accertamento il quarto comma dell'art. 7 prevede che deporrebbe in senso contrario l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia stata condizionata (mediante una c.d. operazione di *tying*) alla prestazione di un consenso a un trattamento, che però non era necessa-

[14] D. Poletti, *op. ult. cit.*, 2784.

rio all'esecuzione di tale contratto[15].

A riprova dell'inequivocità del consenso depone anche il considerando 32 del reg. *GDPR* che prevede che «*il consenso potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle*» [16]. Si richiede quindi un comportamento attivo o una esplicita manifestazione di volontà.

Il legislatore europeo oblitera dunque il modello del consenso ottenuto mediante un procedimento di *opt-in*, e non con una opzione preselezionata da deselezionare (*opt-out*) che non può costituire esplicita manifestazione di volontà. In proposito, la Corte di Lussemburgo, sul caso *Planet 49* [17], ha statuito che l'uso di una casella preselezionata non consente di dedurre che l'utente di un sito *web* abbia prestato un consenso inequivoco di una sua accettazione all'installazione dei *cookies*. Quando l'utente si trovi dinanzi a una casella che contenga già il *flag* di accettazione all'installazione dei *cookies*, la Corte non è in grado di escludere che il soggetto possa non avere letto la didascalia posta a fianco della casella o possa non averla neppure vista.

Di recente, la Corte di giustizia, con la sentenza dell'11 novembre 2020 sul caso *Orange Romania*, C-61/19 [18], in continuità con il proprio precedente sul caso *Planet 49*, C-673/17, ha fornito indicazioni di rilievo sulla validità del consenso al trattamento e sulla prova della sua esistenza da parte del ti-

[15] In proposito, anche se relativa a una pratica di *tying* precedente all'entrata in vigore del reg. *GDPR*, si veda Cass. civ., 2 luglio 2018, n. 17278, in *Nuova giur. civ. comm.*, 2018,12, 1775 ss., con nota di F. Zanovello, *Consenso libero e specifico alle e-mail professionali*, e in *Giur. it.*, 2019, 3, 530 ss., con nota di S. Thobani, *Operazioni di* tying *e libertà del consenso*, in *Giur. it*., 2020, 1, 79 ss.

[16] Sul punto C. Basunti, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, cit., 874.

[17] Corte giust., 1 ottobre 2019, C-673/17, con commento di S. El Sabi, *La Corte di Giustizia vieta le caselle di spunta preselezionate per il consenso all'uso dei* cookie, in *Giustiziacivile.com*, 19 febbraio 2020, e da A. Reinalter-S. Vale, *Cookie e consenso dell'utente*, in *Giur. it*., 2020, 1, 79 ss.

[18] Corte giust., 11 novembre 2020, C-61-19, con commento di 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 leggi civ. comm.*, 1/2021, 247 ss.

tolare del trattamento [19]. I Giudici di Lussemburgo erano stati chiamati a interpretare il rinvio del giudice nazionale relativamente alla questione dell'idoneità di un contratto di fornitura di servizi di telecomunicazioni a dimostrare valida prestazione di consenso al trattamento dei dati personali, ove contenesse una clausola secondo cui l'interessato era stato informato e aveva acconsentito al trattamento di alcuni dati personali per determinate finalità.

La Corte afferma che la prova di un valido consenso al trattamento spetti al titolare del trattamento e che le clausole contrattuali secondo cui l'interessato ha prestato il consenso al trattamento di alcune categorie di dati per determinate finalità, non possono rendere inequivoca dimostrazione che l'interessato abbia validamente manifestato il proprio consenso. Conseguentemente per la Corte non basta la preselezione di una casella "di spunta", che riguardi una clausola relativa alla prestazione del consenso, per provare un consenso inequivoco del titolare del trattamento. L'informazione fornita deve infatti essere accessibile e deve consentire all'interessato di individuare agevolmente le conseguenze del consenso prestato, in modo da assicurare che il consenso prestato sia una determinazione consapevole. La Corte europea pertanto dichiara l'insussistenza di un'effettiva autodeterminazione dell'interessato in due ipotesi: *a*) laddove le clausole contrattuali possano indurre l'interessato in errore circa la possibilità di stipulare il contratto anche in caso di mancanza del consenso, e dunque quando si subordini la prestazione di un servizio al consenso al trattamento dei dati; oppure *b*) qualora il titolare del trattamento esiga che la persona interessata, per rifiutare il proprio consenso, compili un modulo supplementare che ne attesti tale rifiuto.

Tornando poi all'analisi della disciplina del regolamento europeo, conformemente poi a quanto previsto dal terzo comma dell'art. 7, l'interessato ha poi il diritto di revocare il proprio consenso in qualsiasi momento, senza

[19] Il caso riguardava la fornitura di servizi di telefonia ai clienti ad opera dell'impresa *Orange Romania*. La società telefonica aveva concluso in forma scritta alcuni contratti contenenti una clausola in cui si dichiarava che l'interessato era stato informato del trattamento dei dati personali contenuti nelle copie dei documenti d'identità, allegati alla documentazione negoziale, e che ne aveva prestato consenso. A ben vedere la *Orange Romania* non subordinava la fornitura del servizio telefonico alla prestazione del consenso al trattamento dei dati, ma esigeva in alcuni contratti di abbonamento che la persona interessata, per rifiutare il proprio consenso, compilasse un modulo supplementare in grado di attestarne il dissenso.

che con ciò si pregiudichi la liceità del trattamento basata sul consenso prima della revoca.

Una specifica previsione è inoltre dettata dall'art. 8 reg. *GDPR* per l'offerta ai minori di servizi della società dell'informazione. In tal caso il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni, ma gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

L'esposta disciplina non sempre consente di fornire conclusioni univoche in ordine a una delle più controverse questioni sollecitate dalla disciplina europea, ossia la natura del consenso dell'interessato. In argomento si riscontrano tradizionalmente due opzioni ermeneutiche: *a*) la tesi della natura non negoziale [20], perché il diritto alla riservatezza del dato personale costituisce un diritto indisponibile, in quanto diritto della personalità, rispetto al quale il consenso è un'autorizzazione, che ha funzione scriminante di un'attività che altrimenti sarebbe illecita. E in tal senso deporrebbe non soltanto l'ascrivibilità del consenso a una delle possibili condizioni di liceità, ma anche la possibilità che il consenso espresso dell'interessato consenta di superare il divieto di trattamento di dati sensibili, biometrici e genetici (art. 9, par. 2, lett. *a*), reg. *GDPR*); *b*) di contro, la tesi della natura negoziale [21], che intende le informazioni oggetto di trattamento come protagoniste di un processo di reificazione, all'esito del quale assumono i connotati di beni giuridici, rispetto ai quali il consenso assumerebbe funzione dispositiva. E in tal senso, nonostante le numerose condivisibili obiezioni ad applicare la logica proprietaria ai dati personali [22], si valorizzerebbe me-

[20] In tal senso, tra i tanti, D. Messinetti, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, 339 ss., spec. 350; S. Patti, *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civ.*, 1999, II, 466 s.

[21] In proposito G. Oppo, *Sul consenso dell'interessato*, in *Trattamento dei dati personali e tutela della persona*, a cura di V. Cuffaro-V. Ricciuto-V. Zeno Zencovich, Milano, 1998, 118 ss.; nonché V. Zeno Zencovich, *Una lettura comparatistica della l. 675/96 sul trattamento dei dati personali*, *ivi*, 169.

[22] Di tutta evidenza che con il consenso dell'interessato al trattamento dei dati personali non vi sarebbe effetto traslativo ai sensi dell'art. 1376 c.c., perchè l'interessato manterrebbe la titolarità del dato personale. Come osservato da G. Resta, *Autonomia privata e diritti della personalità*, Napoli, 2005, il regime di circolazione del dato personale è connotato dalla persistenza di un in-

glio l'autodeterminazione individuale, sottesa ad esempio all'atto di accesso al *web*, che come è stato osservato parrebbe «*tradursi in un comportamento concludente attraverso il quale l'interessato manifesta la propria disponibilità affinché altri raccolgano ed elaborino le proprie informazioni*» [23]. In senso proclive al secondo orientamento muoverebbe anche la considerazione che difficilmente l'attività di trattamento dei dati potrebbe essere considerata come illecita per sua natura [24].

Tra le due chiavi di lettura del consenso – o come atto di autorizzazione nell'ottica della tutela della persona o come elemento di una fattispecie negoziale, in linea con la crescente negoziabilità del dato – a ben vedere, non è facile propendere per una soluzione netta.

È indubbio che la revoca del consenso sia retaggio dell'intendere il consenso come autorizzazione alla lesione della propria sfera personale e mal si concilierebbe con la qualificazione negoziale che ravvisa nel consenso dell'interessato la cessione del dato da parte dell'interessato al titolare, perchè il vincolo una volta sorto sarebbe irretrattabile dalle parti [25]. Eppure il movimento in atto sul terreno dei diritti della personalità, che si aprono all'autonomia privata, dismettendo quel tradizionale carattere dell'indisponibilità, veicola forme di patrimonializzazione del diritto della persona e, segnatamente, di sfruttamento ad opera del titolare [26], conciliabili con una lettura negoziale del consenso. L'inclusione dei dati personali nel perimetro dell'oggetto contrattuale, fungendo sostanzialmente da controprestazione,

cisivo potere di controllo sulle modalità di utilizzazione della risorsa ben oltre il primo atto di disposizione del diritto. Non un consenso traslativo, dunque. Semmai il consenso costituirebbe un atto di assenso all'altrui ingerenza nella propria sfera giuridica, che genera obblighi di comportamento sia in capo all'interessato, sia in capo al titolare del trattamento. Così S. Sica, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Riv. dir. civ*., 2001, 633 ss.

[23] F. Caggia, *Libertà ed espressione del consenso*, in *I dati personali nel diritto europeo*, a cura di V. Cuffaro-R. D'Orazio-V. Ricciuto, cit., 255.

[24] In tal senso S. Mazzamuto, *Il principio del consenso e il problema della revoca*, cit., 1028.

[25] F. Caggia, *Libertà ed espressione del consenso*, cit., 269.

[26] In proposito, tra i tanti, si veda G. Resta, *Autonomia privata e diritti della personalità*, cit.; A. Nicolussi, voce *Autonomia privata e diritti della persona*, in *Enc. dir.*, Ann. IV, Milano, 2011, 133 ss.; e, più di recente, A. De Franceschi, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017; S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Torino, 2019.

assume poi ampio risalto specie dinanzi a quelle operazioni contrattuali che – frequenti in tempi recenti – riguardano trattamenti massivi di dati personali. In proposito, vengono a mente le riflessioni di Stefano Rodotà, nell'osservare che «*dobbiamo lavorare molto nella dimensione negoziale, non ho nessun dubbio. Negoziale vuol dire per esempio: il consenso può essere oneroso, può essere condizionato, può essere a termine? Io come risposta generale direi di sì (…) 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 in parte, dimostrano quindi che c'è una scelta dell'interessato che definisce l'area della protezione*» [27].

In tal senso allora che il consenso possa rivestire carattere negoziale non costituisce per forza adesione a una visione improntata alla piena disponibilità dei dati personali o per abdicare alla sponda personalistica, ma per valorizzare quel controllo dell'atto di autonomia privata in funzione della salvaguardia dei valori della persona che risultano coinvolti [28].

2.2. – La breve ricognizione della disciplina del consenso dell'interessato, contenuta nel regolamento europeo del 2016, delinea una parabola discendente della centralità del consenso dell'interessato rispetto al trattamento dei dati personali.

Indice di una tale tendenza non è soltanto l'emersione di ulteriori condizioni di liceità del trattamento a prescindere dal consenso, ma come si è esaminato anche l'impossibilità per l'interessato di incidere sulle modalità e sulla scelta dei mezzi del trattamento, rimesse piuttosto alla valutazione del titolare del trattamento. E la perdita di centralità del consenso non è solo il riflesso dell'adozione della prospettiva del titolare in luogo di quella dell'interessato, ma risiede anche nel consenso "forzato", che per accedere a un bene e a un servizio è richiesto all'interessato [29]. Colui che intende accedere a un

[27] Così S. Rodotà, *Conclusioni*, in *Trattamento dei dati personali e tutela della persona*, a cura di V. Cuffaro-V. Ricciuto-V. Zeno Zencovich, cit., 308, come ricordato anche da V. Ricciuto, *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-V. Ricciuto, cit., 29 s.

[28] F. Piraino, *I "diritti dell'interessato" nel Regolamento generale sulla protezione di dati personali*, cit., 2786.

[29] Sul punto, V. Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, cit., 38 ss.

servizio o acquisire un bene tramite transazioni commerciali, quando si tratta di beni e servizi fortemente connessi al trattamento dei dati di chi ne li intende acquistare, si ritrova costretto a disporre di quei dati personali, cedendoli. In tal modo, il consenso prestato non è del tutto libero, perché non costituisce una scelta autonoma dall'acquisto del bene e del servizio, né è prevista una compensazione economica per la cessione del dato personale, nonostante spesso l'accesso al servizio o l'acquisto del bene abbiano un valore inferiore rispetto al "prezzo" del consenso [30]. A ben vedere una siffatta situazione di consenso "forzato" potrebbe ricorrere quando esso è reso sia "in occasione" o "in vista" di beni e servizi (es. il diritto all'accesso e all'uso di un social, la possibilità di utilizzare un motore di ricerca) sia "in ragione" dell'ottenimento di beni e servizi (es. la possibilità di utilizzare una certa *app* che richiede l'utilizzo di certi dati personali, senza la cessione dei quali non vi potrebbe essere la prestazione del servizio). Il consenso al trattamento può quindi rivelarsi strumentale allo svolgimento della fase precontrattuale o all'esecuzione di un contratto. In queste circostanze si osserva il ricorrere di una forte disparità di potere contrattuale, riflesso della naturale vocazione della società allo sviluppo delle tecnologie informatiche [31].

Occorre oltretutto considerare che dinanzi a reiterate richieste di consenso da parte delle *data companies* si assiste a una riduzione della soglia di attenzione dell'interessato, anche dinanzi all'informativa al trattamento, con conseguenze in ordine alla capacità cognitiva dell'interessato, tali da compromettere l'integrità del processo decisionale che precede il consenso al trattamento.

Le interferenze tra consenso e contratto, allora, non possono confluire in una inequivoca conclusione positiva sulla ammissibilità di ogni prestazione di consenso contenuta nel contratto. Lo si desume dalla recente soluzione accolta dalla Corte di giustizia sul caso *Orange Romania*: il testo contrattuale non deve forzare il consenso, subordinando il servizio alla prestazione di esso o inducendo in errore l'interessato sulla possibilità che il suo rifiuto al tratta-

[30] In proposito G. Resta-V. Zeno Zencovich, *Volontà del consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ*., 2018, 411, che – criticando il richiamo alla categoria delle obbligazioni naturali per la ricostruzione del fenomeno di circolazione dei dati personali – mettono in risalto il grande rilievo giuridico-economico delle operazioni di trattamento dei dati personali compiute da *data companies* del calibro di *Google* e *Facebook*.

[31] V. Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, cit., 38.

mento dei dati non comprometta la prestazione di un servizio ad opera dell'altro contraente [32].

Le esposte considerazioni nella direzione di una perdita di centralità del consenso – tendenza arginata dalle menzionate pronunce della Corte di giustizia – si accompagnano alla constatazione che la revoca del consenso dell'interessato potrebbe costituire talvolta uno strumento svuotato di effettività. Si pensi a una circolazione dei dati che ormai è divenuta virale nella rete e sfugge quindi alla possibilità che il titolare ne arresti la circolazione, riacquistandone la signoria, senza contare i casi in cui essa sia inibita – al tempo della *Personal Data Economy* (c.d. *PDE*) – dall'avere ceduto contrattualmente il dato personale.

La dequotazione del consenso si traduce inevitabilmente nella necessità di riattribuire al consenso la sua funzione di meccanismo di partecipazione e di decisione dell'interessato al trattamento dei dati personali, che tuttavia abbia in conto il carattere massivo e pervasivo dei trattamenti nel contesto contemporaneo, «*collocandosi oltre una prospettiva esclusivamente individuale*» [33].

2.3. – Una positivizzazione dello schema di cessione del dato personale campeggia nella direttiva 2019/770/UE (*Digital Content and Service Directive,* c.d. *DCSD*), che ha disciplinato alcuni aspetti dei contratti di fornitura e di servizi digitali [34]. La direttiva, all'art. 3, par. 1, nell'individuare l'ambito applicativo, prevede che la cessione di un dato personale possa costituire

[32] 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*, cit., 264.

[33] C. Angiolini, *op. ult. cit.*, 266.

[34] Uno stimolo all'interazione tra la protezione dei dati personali e il contratto era stato già apprestato - nel travagliato *iter* che ha portato alla *DCSD* – dalla proposta di direttiva 2015/0287/UE, che tuttavia – all'art. 3 – conteneva una equiparazione del pagamento mediante dati personali con quello mediante moneta. Una tale formulazione letterale che conferiva ai dati personali carattere di forma di pagamento sostitutiva rispetto a quella mediante denaro è stata poi abbandonata anche in considerazione dell'opinione (n. 4/2017) dell'Autorità Garante europea sulla protezione dei dati personali (*EDPB*), critica a una previsione che sottendesse una "mercificazione" del dato personale. L'Autorità europea aveva ritenuto infatti – alla nota 27 della menzionata opinione - che espressioni come "moneta digitale" o "pagamento per mezzo dei dati personali" non soltanto si dovessero considerare fuorvianti, ma addirittura pericolose («*"Popular catchphrase like "digital currency" and "paying with data" may not only be misleading, but can also be dangerous, if it is taken literally and turned into a legal principle*»).

controprestazione per la fornitura di contenuti o servizi digitali da parte di un operatore economico [35]. In questo caso colui che cede il proprio dato personale è consumatore di un contenuto e servizio digitale, senza versare in cambio alcun corrispettivo pecuniario [36].

Il considerando 24 della stessa *DCSD* prevede che il consumatore, quando non paghi un prezzo per la fornitura di contenuti digitali o di servizi digitali, fornisca dati personali all'operatore economico. A fronte del frequente utilizzo nel mercato di tali modelli commerciali che tuttavia non possono declassare a merce il diritto fondamentale dell'interessato sul dato personale, la menzionata previsione normativa si prefigge di garantire che i consumatori abbiano diritto a rimedi contrattuali per la protezione dei dati personali forniti all'operatore economico al momento della conclusione del contratto o successivamente. Ad esempio, la presente direttiva dovrebbe applicarsi nel caso in cui il nome e l'indirizzo email forniti da un consumatore al momento della creazione di un *account* sui *social media* siano utilizzati per scopi diversi dalla mera fornitura di contenuti digitali o servizi digitali o non conformi agli obblighi di legge o, ancora, nel caso in cui il consumatore acconsenta a che il materiale che provvede a caricare (e che contiene dati personali, come fotografie o *post*) sia trattato a fini commerciali dall'operatore economico.

L'apporto fornito dalla *DCSD* è quello di avere provveduto a un avvicinamento della disciplina della protezione dei dati personali allo statuto consumeristico, in modo da implementare il potenziale rimediale a disposizione del consumatore-interessato (come ad esempio dinanzi alle pratiche commerciali scorrette) [37].

La positivizzazione dello schema negoziale di cessione del dato personale investe un ruolo non marginale sul consenso dell'interessato, confermando la tendenza in atto, che attrae il consenso nelle dinamiche negoziali di atti di-

[35] L'art. 3, par. 1, direttiva 2019/770/UE (*DCSD*) prevede che «*la direttiva è applicabile 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*».

[36] G. Marino, Internet *e tutela dei dati personali: il consenso ai* cookie, in *Jus civile*, 2/2020, 399 s.

[37] G. Marino, *op. ult. cit.*, 424 ss.

spositivi per la fornitura di beni o servizi a contenuto digitale, in luogo di quell'originaria valenza a costituire un atto di tolleranza dell'ingerenza alla propria sfera personale. Si osserva tuttavia che nell'attuale società interconnessa, la considerazione dei dati personali quale risorsa destinata alla circolazione su scala globale, non può trascurare la centralità della persona umana «*la cui tutela non può essere obliata dalla mera rilevanza economica delle proprie informazioni*» [38].

2.4. – Alle dinamiche di cui si è dato conto si accompagna un consenso che – per attuare la specificità del consenso dell'interessato, prevista nella definizione dell'art. 4 n. 11 *GDPR* (e della previsione normativa previgente) – diviene "granulare". Il consenso è specifico quando è mirato in relazione a un trattamento o in relazione alle finalità o in relazione a un dato al quale esso è preordinato. Da qui la possibilità per l'interessato di prestare il proprio consenso: *a*) non estendendolo a taluni trattamenti; *b*) nell'ambito di taluni trattamenti, escludendolo per alcune finalità; *c*) pur ammettendo un trattamento per una o più finalità, sottraendo alcuni dati al trattamento.

Conseguentemente, per il titolare del trattamento di dati degli utenti è necessario creare differenti richieste a seconda delle diverse finalità di trattamento dei dati personali: ad esempio è necessaria una richiesta distinta qualora si richieda il consenso a ricevere aggiornamenti sulle attività e sulla pubblicazione di *post* sul *web* o a ricevere comunicazioni promozionali ed inviti ad eventi o promozioni speciali, dunque per finalità di *marketing*.

Il nuovo volto "granulare" del consenso è stato avallato di recente dalle Linee guida del 4 maggio 2020 (n. 5/2020), adottate in materia di consenso dallo *European Data Protection Board* (*EDPB*), l'Autorità garante europea nella quale confluiscono le autorità nazionali di protezione dei dati personali. Con un aggiornamento rispetto alla versione già adottata il 10 aprile 2018, l'Autorità europea ha tentato di recuperare il rilievo del consenso, affrontando le problematiche concernenti l'accettazione dei *cookies* di un sito *web* da parte dell'utente, ossia di tutte quelle informazioni immesse sul *browser* degli

[38] C. Basunti, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, cit., 893.

utenti [39], quando essi navigano su internet tramite pc, *tablet* o *smartphone* [40]. In tutti questi casi l'utente deve prestare il proprio consenso all'uso dei *cookies*, altrimenti gli sarà precluso l'accesso al sito *web*. In questi casi non saranno sufficienti per prestare il consenso da parte dell'interessato né lo scorrimento di una pagina *web* per "eliminare" il *banner* che si presenta all'ingresso utente (c.d. *scrolling*), né l'attività minima (ad es. un movimento del cursore) con cui l'interessato dà parvenza di avere fornito il proprio consenso senza una reale consapevolezza del trattamento (c.d. *swiping*): entrambe le tecniche non assicurerebbero un consenso esplicito e inequivocabile, in linea con la citata giurisprudenza della Corte di giustizia, che ribadisce il modello dell'*opt-in*, reprimendo la prassi della preselezione delle caselle di spunta. Orbene, se la "granularità" del consenso consentirebbe di manifestare la volontà dell'interessato in riferimento soltanto a specifiche finalità, potendo escluderne altre, sono altresì preclusi dalle Linee guida i c.d. *cookie wall*, ossia quei banner che presentano la scelta tra l'installazione in blocco di tutti i *cookie* oppure la rinuncia all'accesso. In questi casi l'interessato si trova davanti a un "muro" che, con palese alterazione della sua libera capacità di autodeterminazione, condiziona la fruizione del servizio alla positiva autodeterminazione al trattamento dei suoi dati.

3. - Il dato personale all'epoca di un'economia digitale, come si è anticipato, costituisce un imprescindibile fattore di sviluppo delle nuove economie globali. La distribuzione di beni e servizi capillare e planetaria e l'irriducibilità del mercato di riferimento a un definito ambito geografico contribuivano già alla "deterritorializzazione" del commercio (e, più nel complesso, delle relazioni sociali), ossia a una rarefazione dell'aspetto geografico di svolgimento di un'attività economica, che si disloca piuttosto in uno spazio (o una dimensione) "virtuale". Un irrinunciabile uso della rete e di nuove tecnologie

[39] I *cookie* costituiscono *file* di testo che il fornitore di un sito *internet* installa nel *computer* dell'utente che lo abbia visitato, al quale potrà accedere durante una nuova navigazione sullo stesso sito da parte di quel medesimo utente. Si suole distinguere tra *cookie* tecnici, che sono installati dai titolari o gestori del sito *web* per consentire un migliore accesso o una più agevole navigazione, e *cookie* di profilazione, che sono installati dai gestori del sito *web* o da *data companies* per creare un *identikit* dell'utente durante la sua navigazione in rete, attraverso l'utilizzo di algoritmi di calcolo.

[40] G. Marino, Internet *e tutela dei dati personali: il consenso ai* cookie, cit., 398 ss.

digitali, specie al tempo dell'emergenza sanitaria da *Covid-19*, ha confermato la rilevanza per le organizzazioni complesse di gestire i dati analitici degli utenti per ricavarne informazioni utili ai loro processi decisionali, ossia l'impiego di quelle tecniche di elaborazione delle informazioni basate sui *big data* [41].

Com'è noto, questa vasta mole di informazioni è raccolta ed elaborata secondo il "*paradigma delle 3 V*", ossia *volume*, *velocità* e *varietà*: il trattamento di un siffatto aggregato informativo si caratterizza per la capacità di processare una vasta quantità di dati (*volume*), suscettibile di una capacità di crescita esponenziale (*velocità*) e di riguardare una congerie di formati di dati differenti tra loro (*varietà*). Quel che più interessa al giurista, rispetto alle connotazioni quantitative e qualitative dell'aggregazione, è la capacità di generare nuove informazioni, ossia di trarre da quei flussi di dati sempre più informazioni predittive, tali da individuarne le traiettorie di propagazione e da prevedere le tendenze future [42]. Attraverso dunque tutte quelle tracce lasciate online da un utente (*cookies*, *email*, *click* nel *browser* ecc.) è ben possibile individuare *trend* di consumo, comportamenti dei singoli e preferenze individuali, funzionali a generare la profilazione dell'utente.

Orbene, proprio per ridurre i rischi di vulnerabilità dell'utente da una sua profilazione, il trattamento concernente *big data analytics* si avvale di alcuni strumenti di sicurezza: tecniche di anonimizzazione (come la generalizzazione o la randomizzazione) e tecniche di pseudonomizzazione (come la crittografia o la tokenizzazione).

Le prime hanno il fine di portare qualsiasi dato personale alla perdita de-

[41] L'origine dei *big data* è correlata allo sviluppo dei *database* relazionali e dei linguaggi di programmazione, e in particolare ai sistemi di *Business Intelligence* (BI) e di *Business Analytics* (BA), che rendono possibile la raccolta regolare e organizzata del patrimonio di dati di un'azienda, da supporto alle decisioni aziendali. La *Business Intelligence* lavora prevalentemente sull'analisi descrittiva, per raccogliere e ordinare dati storici e attuali, in modo da fornire una fotografia della situazione esistente. La *Business Analytics* invece lavora sull'analisi predittiva, attraverso l'elaborazione dei dati tramite i processi di *data mining*, l'analisi statistica dei dati e sistemi di apprendimento automatico, per prevedere i possibili scenari di ciò che accadrà e quindi per adottare le strategie di *business* più idonee in base agli scenari prefigurati. In proposito A. Rezzani, *Architettura, tecnologie e metodi per l'utilizzo di grandi basi di dati*, Milano, 2013; G. D'Acquisto-M. Naldi, Big data *e* privacy by design. *Anomizzazione, pseudonimizzazione, sicurezza*, Torino, 2017.

[42] Tra i tanti, A. Montalero, *La* privacy *all'epoca dei* Big data, cit., 1187.

finitiva dell'elemento identificativo, ad esempio generando distorsioni o alterazioni tali da rendere il dato personale non riconducibile all'utente e, per l'effetto, verrebbe meno la conformità alla definizione di dato personale apprestata dal *GDPR* [43], la cui applicazione sarebbe dunque preclusa. Eppure queste tecniche non risolvono il rischio di una re-identificazione dell'utente.

Viceversa, la pseudonimizzazione permette di mantenere una piena corrispondenza dei dati pseudonimizzati con quelli originari, grazie all'utilizzo di informazioni aggiuntive che riducono la correlabilità del dato con l'interessato e senza alcuna alterazione, in modo da consentire piuttosto ai dati di mantenere il loro valore informativo e di essere sottoposti alla regolazione del *GDPR*, che – all'art. 4 n. 5 – definisce questa tecnica [44].

Prendendo le mosse dalle questioni sulla depersonalizzazione del dato o sulla sua riduzione di correlabilità all'utente per tornare al riflesso sul tema del consenso, il fenomeno della vasta congerie di dati analitici, ormai da tempo noto alla cultura informatica, ingenera il dubbio che l'attuale disciplina europea della protezione dei dati personali non sia sufficiente a superare le criticità sollevate dall'impatto sociale dei *big data* sulla *privacy* dell'interessato, specie sotto il profilo di un'effettiva autodeterminazione del singolo relativamente al trattamento dei dati che su di esso verrà compiuto.

In primo luogo, vi è una difficoltà nel definire preventivamente i possibili impieghi dei dati acquisiti e pertanto le informative fornite agli interessati possono apparire o generiche e vaghe, tradendo la possibilità che quel trattamento sia accompagnato da un consenso specifico, o troppo dettagliate, analitiche e tecniche per essere comprensibili all'interessato. In quest'ultimo caso l'interessato potrebbe disinteressarsi a prendere conoscenza dell'informativa e, conseguentemente, autodeterminarsi in modo scarsamente consa-

[43] L'art. 4 n. 1 intende per "dato personale": «*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*».

[44] L'art. 4 n. 5 definisce la "pseudonimizzazione" come «*il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*».

pevole.

Alla scarsa definizione delle specifiche finalità d'uso delle informazioni che influisce sul consenso, segue poi la difficoltà di assicurare una effettiva portabilità delle informazioni da un operatore a un altro della società dell'informazione, magari perché all'utente non conviene migrare all'altro operatore stante l'incapacità di riprodurre con il nuovo operatore la stessa capacità relazionale (come nel caso della migrazione da un *social network* a un altro, disincentivata per un utente dal fisiologico "effetto rete", in tal caso avente dimensione sociale, con relativa incapacità di aggirare il c.d. *lock-in* sociale) [45].

Proprio nel tentativo di far fronte alle complessità del fenomeno dei *big data*, sprovviste di specifica regolazione giuridica, in data 30 maggio 2017, l'Autorità *antitrust*, l'Autorità garante della comunicazioni e quella per la protezione dei dati personali hanno avviato un'indagine conoscitiva congiunta per meglio comprendere le implicazioni per la *privacy*, la regolazione, la tutela del consumatore e l'*antitrust*, dello sviluppo dell'economia digitale e, in particolare, del fenomeno dei *big data* [46].

Delle riferite criticità il legislatore europeo non dà conto. Come è stato osservato pare infatti «*non avere percepito l'estrema tensione che invece caratterizza l'applicazione del principio di finalità nel contesto dei Big Data, né le criticità che affliggono l'autodeterminazione della persona interessata*» [47]. In questo senso, il *GDPR* costituisce più la prima tappa di un iter ancora da percorrere per approdare a un nuovo modello di regolazione.

Tra le proposte suggerite dalla dottrina figura la proposta di sostituire la specificità del consenso dell'utente alla finalità del trattamento con un'ampia nozione di interesse legittimo, tale da consentire che siano i titolari del trattamento ad effettuare quella valutazione comparativa dei diversi interessi in campo [48]. Per cercare di non indulgere a un eccessivo favore verso gli interes-

[45] Tra i tanti, A. Montalero, *La* privacy *all'epoca dei* Big data, cit., 1187.

[46] L'indagine conoscitiva, dopo svariate audizioni dei principali operatori dell'economia dei dati, delle telecomunicazioni, dei settori finanziari e dell'editoria, nonché esperti e accademici, nonché dopo l'invio di richieste di informazioni ai grandi operatori digitali, si è conclusa con la delibera 458/19/CONS, adottata nel novembre 2019 dall'Autorità garante delle comunicazioni.

[47] Così A. Montalero, *La* privacy *all'epoca dei* Big data, cit., 1192.

[48] L. Moerel-C. Prins, *Privacy for the homo digitalis. Proposal for a new regulatory framework for data protection in the light of Big Data and the Internet of Things*, Tilburg, 2016, 43 ss.

si delle imprese, tuttavia, pare più condivisibile la proposta di prendere atto dell'indeterminatezza dell'uso specifico al momento della raccolta dei dati. Aderendo a questa impostazione si potrebbe sostituire la specificità del consenso per una finalità specifica con una valutazione preventiva dei possibili rischi connessi all'indeterminatezza di un utilizzo specifico. Si tratterebbe di incentivare l'analisi del potenziale pregiudizio che il singolo potrebbe subire da tutti i differenti utilizzi di quei dati, generalizzandola per tutti i trattamenti relativi a *big data*, e non soltanto per alcuni trattamenti (come prevede l'art. 35, par. 3, lett. *a)*, *GDPR*), in luogo quindi dell'acquisizione di un consenso specifico dell'utente interessato. La soluzione prospettata suggerisce il recupero di un modello che però non si presenti come una sorta di autovalutazione da parte dell'interessato, ma recuperi la necessità di un vaglio preventivo da parte dell'autorità di controllo [49]. Una siffatta proposta, laddove non incarni il modello dell'*opt-in*, non può prescindere tuttavia dalla necessità che sia lasciata all'utente la facoltà di esercitare un diritto di opzione a ritirare il consenso manifestato all'esito della valutazione preventiva (*opt-out*) [50].

4. - Al tempo della crescita esponenziale di informazioni generate dall'utente in rete, la disamina sul mutamento di paradigma che il consenso dell'interessato affronta ha posto in evidenza la difficoltà di una composizione organica delle questioni emerse. La tendenza ad abbandonare la logica della protezione di un diritto della personalità per muovere verso la negoziabilità dei dati personali e l'adozione della prospettiva del titolare del trattamento riflettono meglio la progressiva fluidità della circolazione di dati personale, preordinati a una continua riproduzione. Né d'altronde quella progressiva patrimonializzazione dei dati personali, nonostante le problematiche che porta con sé, può essere ostracizzata dal sistema giuridico, mostrando un disallineamento rispetto alle più moderne esigenze di mercato [51]. A questo punto, la regolazione europea della tutela del dato personale mostra da un lato una perdita di centralità del consenso, che non è più l'unica condizione di liceità del trattamen-

[49] Così A. Montalero, *La* privacy *all'epoca dei* Big data, cit., 1193 ss.

[50] L. Moerel, *Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof*, Tilburg, 2014.

[51] C. Basunti, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, cit., 895.

to, compensata dall'altro da una specificazione del consenso in base alle finalità, al trattamento e al dato personale. Ma il principio di un consenso separato (o, meglio, di un consenso "granulare") si rivela, da ultimo, inadatto a cogliere le specificità del fenomeno dei *big data*, che impone una precipua e adeguata risposta normativa, la quale tuttavia non potrà che obliterare quella disillusione – già da tempo ormai manifesta [52] – nei confronti del "mito del consenso".

[52] Era il 1973 quando Stefano Rodotà a proposito dell'impiego di tecniche di elaborazione dei dati redarguiva dal "mito del consenso" (S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, 45 ss.).

Abstract

Il saggio esamina, nel contesto della disciplina europea della tutela dei dati personali, affidata al Regolamento GDPR, le questioni che hanno riguardato il consenso dell'interessato al trattamento, quale veicolo di autodeterminazione e controllo individuale sul trattamento. Tuttavia, dinanzi a una crescente diffusione dei *big data analytics*, funzionali a generare una *mass costumization* dell'utente, si solleva qualche perplessità sull'attitudine dell'attuale regolazione europea (e segnatamente del principio del consenso specifico) a cogliere le peculiarità sottese a questi fenomeni.

The essay examines, in the context of the European data protection law, entrusted to the General Data Protection Regulation (GDPR), the issues which have concerned the consent of the data subject to the data-processing, as a vehicle for self-determination and individual control over the data-processing. However, in front of a growing spread of big data analytics, functional to generate a mass customization of the user, some perplexity arises about the attitude of the current European regulation (and in particular the principle of specific consent) to grasp the peculiarities underlying these phenomena.