JUS CIVILE

Rivista a cura di **Rosalba Alessi, Carmelita Camardi, Massimo Confortini, Carlo Granelli, Mario Trimarchi**

4-2022

luglio-agosto

G. Giappichelli Editore

ISSN 2281-3918/2421-2563

I contributi, inviati alla Rivista per la pubblicazione, sono soggetti a revisione tra pari a doppio cieco (*double blind*). È, quindi, garantito l'anonimato dei valutatori e dei valutati.

Vengono sottoposti a revisione tutti i contributi costituenti Articoli e saggi, inseriti in una delle voci tematiche.

Il Comitato dei revisori è costituito, esclusivamente, da professori ordinari dell'area privatistica, indicati in un apposito elenco pubblicato.

La revisione è affidata a due membri del Comitato dei revisori, scelti a rotazione dai curatori in base alle indicazioni di settore fatte da ciascun componente.

Il *referee* è tenuto a compilare la scheda di valutazione. È garantita la piena autonomia dei revisori rispetto alla Direzione della Rivista.

Soltanto in casi eccezionali, i Curatori assumono, con adeguata motivazione, la responsabilità della pubblicazione.

JUS CIVILE

INDICE

pag.

Articoli e Saggi

[**] I curatori, valutata la rilevanza del contributo, assumono la responsabilità diretta della pubblicazione.

[*] Contributo sottoposto a revisione [*]

JUS CIVILE

JUS CIVILE

pag.

Recensioni

JUS CIVILE

ALESSANDRO PURPURA

Ricercatore di Diritto privato – Università degli Studi di Palermo

IL CONSENSO NEL MERCATO DEI DATI PERSONALI. CONSIDERAZIONI AL TEMPO DEI BIG DATA

SOMMARIO: *1. Premessa. Il "mito" del consenso al tempo dei big data. – 2. Regolazione europea e circolazione del dato personale. – 3. GDPR, primazia del consenso e altre basi giuridiche del trattamento. – 4. La dimensione negoziale del consenso al trattamento. – 5. "Granularità" del consenso e tracciamento della navigazione in rete. – 6.* Segue. *Il caso Orange Romania. – 7. L'apporto della direttiva 2019/770/UE e l'autodeterminazione economica. – 8. Conclusioni. Consenso ed eventuali alternative nella cornice dei big data.*

1. – I mutamenti che ormai da tempo incidono sulla circolazione dei dati personali costituiscono un inesorabile banco di prova della capacità del diritto di adattarsi al progresso tecnologico: l'avvento del nuovo sollecita una domanda di regolazione, che rivela sì la rapida obsolescenza della produzione normativa esistente, ma parimenti consegna all'interprete il delicato ruolo di ricondurla "a sistema", ricercando, secondo logiche proprie del pluralismo giuridico, una matrice comune alle complessità [1]. Da essa muoverebbe il convincimento che esistano «controspinte sufficienti a far pensare che sia ancora possibile un sistema giuridico magari più aperto ma non irrimediabilmente liquefatto» [2].

L'operazione ermeneutica di razionalizzazione – che oltretutto non va esente dai rischi della riconcettualizzazione e della generalizzazione [3] – tuttavia è resa più ardua in quegli ambiti in cui gli esiti dello sviluppo della tecnica, sotto la spinta motrice della globalizzazione, si dispiegano in uno spazio economico, come accade per l'attuale quantità esponenziale di dati personali in circolazione, che induce a trattamenti in massa, nel contesto di un'economia prevalentemente digitalizzata.

Che lo scambio di informazioni sia una costante di ogni rapporto interpersonale [4] lo si evince dalla centralità del diritto alla riservatezza nelle quotidiane relazioni sociali, che impongono quantomeno la declinazione

[1] Così C. CAMARDI, *Certezza e incertezza nel diritto privato contemporaneo*, Torino, 2017, 191 ss., e già M. BARCELLONA, *Critica del nichilismo giuridico*, Torino, 2006, 135 ss.

[2] Così S. MAZZAMUTO, *Il diritto pos-moderno: un concetto inutile o addirittura dannoso?*, in *A proposito del diritto postmoderno, Atti Seminario Leonessa, 22-23 settembre 2017*, a cura di G. GRISI, C. SALVI, *L'unità del diritto*, *Collana del Dipartimento di Giurisprudenza*, XII, *Quaderni del Dottorato*, Roma, 2018, 71.

[3] Rischi avvertiti nel pericolo che un'opera di riconcettualizzazione possa portare con sé una fuga in avanti o che la generalizzazione sia indebita e ceda all'indeterminatezza. In proposito S. MAZZAMUTO, *Il contratto di diritto europeo*[4], Torino, 2020, 21.

[4] Si veda M. FRANZONI, *Lesione dei diritti della persona, tutela della privacy e intelligenza artificiale*, in questa *Rivista*, 2021, 1, 6. Già quasi cinquant'anni fa si osservava che «non si può negoziare la modernità se non continuando a continuamente rivelare informazioni a una pluralità di soggetti» (R. POSNER, *The Right of Privacy*, in *Georgia Law Rev.*, XII, 1977, 3, 393 ss.).

delle proprie generalità, se non qualcosa in più (come per la conclusione di contratti di prestazione di servizi per una qualsiasi utenza o per accedere ad un finanziamento da parte di un istituto di credito o per entrare in certi luoghi, come un circolo o una palestra). In tal modo sarebbe di per sé fisiologica la frizione tra l'esclusività del diritto alla *privacy*, tradizionalmente ascrivibile ai diritti della personalità e dunque dotato di assolutezza, e la "relazionalità" del fenomeno circolatorio.

Ma da qualche tempo utenti e utilizzatori del dato figurano quali soggetti operanti in un mercato [5], in cui si vorrebbe fare del dato personale "oggetto" e, dapprima, partecipe di un processo di reificazione [6], esso viene da più parti rivestito della dignità di "bene", suscettibile di valore economico, per divenire progressivamente merce di scambio di una "*monetary*" o di una "*non monetary*" *transaction* [7]. Non sempre è chiaro se chi propugna tali letture sia pienamente consapevole delle conseguenze sul piano della tutela della persona, ma sono un dato di fatto le spinte a concepire la circolazione dei dati personali come un mercato [8], a testimonianza della sua complessità, oltretutto affidato alla regolazione di un'autorità indipendente. La regolazione della circolazione dei dati personali allora non è orientata solamente alle istanze di tutela della persona titolare del dato, ma si fa carico anche di quelle sottese all'utilizzo del dato personale, fattore di competitività per i soggetti che lo sfruttino [9].

Una distribuzione capillare e planetaria di beni e servizi contribuiva 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 proietta piuttosto in uno spazio "virtuale". L'uso della rete e di nuove tecnologie digitali, massimizzato al tempo dell'emergenza sanitaria da Covid-19, ha accelerato l'impiego di quelle tecniche di elaborazione delle informazioni basate sull'aggregazione di dati analitici, c.d. *big data analytics* [10], ricavati dagli accessi alla rete per la ricerca di un prodotto o servizio a contenuto digitale. Nel solco del modello "postfordista", nel quale il consumatore è partecipe di un processo circolare, in grado di trasformare le esigenze di consumo in fattori di alimentazione della produzione, l'aggregazione dei

---

[5] V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia: elementi per un bilancio ventennale*, in *I dati personali nel diritto europeo*, a cura di V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, Torino, 2019, 20; G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020, 15 ss.

[6] In proposito, tra i tanti, C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, Torino, 2020, *passim*; nonché F. PIRAINO, *Sulla nozione di bene giuridico nel diritto privato*, in *Riv. crit. dir. priv.*, 2012, 3, 459 ss., spec. 464. Cfr. P. PERLINGIERI, *L'informazione come bene giuridico*, in *Rass. dir. civ.*, 1990, 2, 326 ss., poi in *Il diritto dei contratti fra persona e mercato*, Napoli, 2003, 335 ss.

[7] C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, 62; C. ALVISI, *Dati personali e diritti dei consumatori*, in *I dati personali nel diritto europeo*, cit., 1182 ss.

[8] Un mercato che si espone alle sfide descritte in A. QUARTA – G. SMORTO, *Diritto privato dei mercati digitali*, Firenze, 2020, *passim*.

[9] Il considerando n. 30 del regolamento *GDPR* prevede che «le persone fisiche possono essere associate a identificativi *online* prodotti da dispositivi, dalle applicazioni, dagli strumenti e dai prodotti utilizzati, quali gli indirizzi IP, marcatori temporanei (*cookie*) o identificativi di altro tipo, quali i *tag* di identificazione e radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare, se combinate con identificativi univoci e altre informazioni ricevute dai *server*, possono essere utilizzate per creare profili delle persone fisiche e identificarle».

[10] L'origine dei *big data* muove dall'affinamento dei *database* relazionali e dei linguaggi di programmazione, e in particolare ai sistemi di *Business Intelligence* (BI), che si basano prevalentemente sull'analisi descrittiva (per raccogliere e ordinare dati storici e attuali, in modo da fornire una fotografia della situazione esistente), e di *Business Analytics* (BA), che 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, in funzione predittiva). In proposito A. REZZANI, *Architettura, tecnologie e metodi per l'utilizzo di grandi basi di dati*, Milano, 2013, *passim*; G. D'ACQUISTO, M. NALDI, *Big data e privacy by design. Anomizzazione, pseudonimizzazione, sicurezza*, Torino, 2017, *passim*; A.C. NAZZARO, *L'utilizzo dei Big data e i problemi di tutela della persona*, in *Rass. dir. civ.*, 2018, 4, 1239 ss.

dati è funzionale a profilare gli utenti [11], individuandone le preferenze, specialmente quelle di consumo, mediante algoritmi di *machine learning*.

Il mercato digitale affronta dunque nuove sfide: dapprima con il c.d. "*web* 2.0", che agevola l'insorgere di posizioni monopolistiche, che trasformano il *web* in un complesso di piattaforme» con interazione diversificata (come *Facebook*, *Twitter*, *Instagram*, ecc.) [12]; e da ultimo con l'ambizioso traguardo del c.d. "*web 3.0*" [13], che propone ulteriori livelli di integrazione della rete, attraverso strumenti innovativi. Tra questi: *a*) la semantica dei dati, per permettere ricerche più accurate, (proponendosi la sfida di un "*semantic web*", immaginabile grazie a elaboratori capaci di una lettura simultanea di tutti i dati del *web*); *b*) l'intelligenza artificiale, che mediante il ricorso ad archivi di dati individua necessità e gusti degli utenti secondo il loro comportamento in rete; *c*) l'utilizzo di nuovi algoritmi, volti alla costruzione di ambienti più complessi (tridimensionali), grazie a maggiori capacità di calcolo. Ambienti sempre più intelligenti aumentano l'identificabilità di un dato conferendo valore semantico a quel che prima appariva un'informazione rappresentata da una certa quantità di segni [14].

Si registra, dunque, la tendenza a cogliere in qualsiasi informazione relativa all'attività sul *web* dell'utente, conformemente alla definizione di cui all'art. 4, n. 1, reg. *GDPR*, un'attitudine "identificativa" della persona fisica [15]. E questa capacità di per sé giustificherebbe la permanenza della riservatezza del dato personale nel novero dei diritti della personalità [16]. Semmai la produzione esponenziale e, il più delle volte, inconsapevole di informazioni nelle attività sul *web* indurrebbe a ritenere che i *big data* non sempre consistano in veri e propri dati personali, ma, «in senso metaforico, elementi più vicini alle c.d. *res derelictae*, di cui chiunque può appropriarsi» [17]. E quindi la vocazione "aperta" della nozione di dato personale, che ricomprende un enorme numero di situazioni tra loro eterogenee e non sempre prevedibili al diritto, veicolate dall'utilizzo della nuova tecnologia *web 3.0*, mette in crisi la stessa utilità di una definizione unitaria rispetto alla finalità di tutela alla quale è preordinata [18].

---

[11] L'art. 4, n. 4, del regolamento *GDPR* intende per "profilazione": «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

[12] A. QUARTA, *Mercati senza scambi. Le metamorfosi del contratto nel capitalismo della sorveglianza*, Napoli, 2020, spec. cap. II.

[13] Cfr. R. DUCATO, *La crisi della definizione di dato personale nell'era del web 3.0. Una riflessione civilistica in chiave comparata*, in *Le definizioni nel diritto*, *Atti delle giornate di studio 30-31 ottobre 2015, Università di Trento*, a cura di F. CORTESE, M. TOMASI, Trento, 2016, *passim*.

[14] H. ZECH, *Information as a property*, in *Journal of Intellectual Property*, *Information technology ad Electronic Commerce Law*, 2015, 6(3), 192.

[15] Si richiama la definizione di dato personale espressa dall'art. 4, n. 1, reg. *GDPR*, secondo la quale per dato personale si intende «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».

[16] Sui diritti della personalità, A. DE CUPIS, *Diritti della personalità*[2], *Tratt. dir. civ. comm*., diretto da A. CICU, F. MESSINEO, L. MENGONI, Milano, 1982, 38 ss.; D. MESSINETTI, voce *Personalità (diritti della)*, in *Enc. dir.*, XXXIII, Milano, 1983, 355 ss.; P. RESCIGNO, voce *Personalità (diritti della)*, in *Enc. giur. Treccani*, XXIV, Roma, 1991, 1 ss.; V. ZENO ZENCOVICH, voce *Personalità (diritti della)*, in *Dig. disc. priv., sez. civ.*, XIII, Torino, 1995, 436 ss.; P. PERLINGIERI, *La persona e i suoi diritti. Problemi del diritto civile*, Napoli, 2005, *passim*; D. MESSINETTI, *L'autodeterminazione dispositiva della persona e il valore di libertà del soggetto*, in *Riv. crit. dir. priv.*, 2008, 547 ss.; G. ALPA, G. RESTA, *Le persone fisiche e i diritti della personalità*, in *Tratt. dir. civ.*, a cura di R. SACCO, Torino, 2019, spec. 453 ss.

[17] M. FRANZONI, *Lesione dei diritti della persona, tutela della privacy e intelligenza artificiale*, cit., 11.

[18] Un rischio della generalizzazione a livello definitorio potrebbe consistere sia nel porre sullo stesso piano dati soggetti ad "ano-

L'elaborazione automatizzata dei dati acquisiti attraverso gli strumenti informatici consente, dunque, un più agevole raggruppamento degli utenti in classi omogenee per gusti, interessi e comportamenti, così da trarne previsioni sulle future determinazioni [19], in modo da orientare le strategie commerciali dei principali attori del mercato (ad esempio, mediante annunci pubblicitari personalizzati). Sullo sfondo della tecnica della c.d. *mass customization* si osserva una nuova stagione, di *orwelliana* memoria: un capitalismo c.d. "della sorveglianza" [20], preordinato alla captazione delle scelte degli utenti (preferenze, interazioni, stili di vita) per poi poterle indirizzare, quale flusso di ritorno di un monitoraggio predittivo. Questi atteggiamenti, sintomatici della capacità delle imprese di adattarsi alle sfide poste dalla rivoluzione digitale, hanno consentito l'affermarsi di strategie imprenditoriali "estrattive", che ottengono enormi ricavi grazie all'impiego di risorse acquisite con costi – laddove vi siano – infinitesimali, in quanto cedute senza alcuna percezione da parte degli interessati della loro reale portata economica [21].

Al passo con quella tendenza alla patrimonializzazione dei diritti della persona [22] e nella suggestione che i dati personali si rivelino un "nuovo petrolio" [23], dal dato è dunque ricavabile un indice di propensione al consumo, una possibile convergenza della persona al consumo, che porta all'emersione della componente economica del dato personale, a scapito di quella etico-esistenziale, che era valsa all'elaborazione di un diritto fondamentale della persona (*ex* art. 8 CEDU) [24]. D'altronde al rilievo autonomo delle dimensioni esistenziale e patrimoniale, smentito dai tempi, pare sostituirsi un'inscindibile compenetrazione, che assume la persona umana nella sua considerazione unitaria, come fattore di agglu-

---

nimizzazione", "pseudonimizzazione" o "deidentificazione", sia nel lasciare sprovvisti di tutela dati grezzi (*raw*) che non consentono un'immediata identificabilità per la mente umana, ma possono acquisire significato laddove sottoposti al trattamento degli elaboratori elettronici, e in tal caso la scarsa probabilità di identificazione potrebbe essere nel tempo superata dallo sviluppo tecnologico. In proposito, si vedano N. PURTOVA, *The law of everything. Broad concept of personal data and future of EU data protection law*, in *Law, Innovation and tecnology*, 2018, 40 ss.; R. DUCATO, *La crisi della definizione di dato personale nell'era del web 3.0.*, cit., *passim*; E. PELLECCHIA, *Dati personali, anonimizzati, pseudonimizzati, deidentificati: combinazioni possibili di livello molteplici di identificabilità nel GDPR*, in *Nuove leggi civ. comm*., 2020, 360 ss.

[19] A. MANTALERO, *La privacy all'epoca dei Big data*, in *I dati personali nel diritto europeo*, cit., 1187.

[20] S. ZUBOFF, *Il capitalismo della sorveglianza*, trad. it., Roma, 2019, *passim*; G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, cit., 11 ss.; AA.VV., *Mercati senza scambi. Le metamorfosi del contratto nel capitalismo della sorveglianza*, cit., *passim*. In proposito anche A. QUARTA, *Capitalismo cognitivo*, a cura di C. VERCELLONE, Roma, 2006, *passim*; A. FUMAGALLI, *Bioeconomia e capitalismo cognitivo. Verso un nuovo paradigma di accumulazione*, Roma, 2007, *passim*; V. CODELUPPI, *Il biocapitalismo*, Torino, 2008, *passim*.

[21] 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.*, 2019, 12, 2799, che richiama, a proposito del capitalismo "estrattivo", S. SASSEN, *Espulsioni. Brutalità e complessità nell'economia globale*, Bologna, 2015, *passim*.

[22] In proposito, *ex multis*, si vedano G. RESTA, *Autonomia patrimoniale e diritti della personalità*, Napoli, 2005, *passim*; ID., *Contratto e persona*, in *Tratt. dir. priv.*, diretto da V. ROPPO, IV, *Interferenze*, a cura di V. ROPPO, Milano, 2006, 2 ss.; F.G. VITERBO, *Protezione dei dati personali e autonomia negoziale*, Napoli, 2008, 9 ss.; A. NICOLUSSI, voce *Autonomia privata e diritti della persona*, in *Enc. dir.*, Ann. IV, Milano, 2011, 133 ss.; C. MIGNONE, *Identità della persona e potere di disposizione*, Napoli, 2014, *passim*; S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Torino, 2019, *passim*; L. VALLE, *Il contratto e la realizzazione dei diritti della persona*, Torino, 2020, *passim*; G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, cit., *passim*, spec. 27 ss. e 113 ss.

[23] Lo si evince, ad esempio, dal documento "*Personal Data. The Emergence of a New Asset Class*" del gennaio 2011 del "*World Economic Forum*" (WEF), pubblicato il 17 febbraio 2011 su *Weforum.org*, dal quale si legge che «*personal data will be the new "oil" – a valuable resource of the 21st century. It will emerge as a new asset class touching all aspects of society*». In proposito C. BASUNTI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contr. impr*., 2020, 2, 862. Cfr. M. GAMBINI, *Dati personali e internet*, Napoli, 2008, 24 ss.

[24] Si veda R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contr. e impr.*, 2020, 760 ss. Cfr. A. DE FRANCESCHI, *La circolazione dei dati tra privacy e contratto*, Napoli, 2017, 12.

tinamento, volto a mitigare la netta separazione tra la sfera patrimoniale e quella non patrimoniale [25].

Alla forza propulsiva delle dinamiche osservate non è estraneo il consenso dell'interessato, snodo cruciale tra la persona, la sua proiezione all'esterno e l'incidenza del terzo, sollecitata dalla circolazione o commercializzazione del dato personale. Finché la protezione del dato personale è tutela del nucleo non patrimoniale del diritto, della sfera privata e personale di ciascun individuo, il consenso è autodeterminazione individuale che incide, da ultimo, sulla realizzazione della personalità umana e sulla sua salvaguardia da interferenze esterne. Ma non appena la protezione dei dati personali perda l'originaria vocazione esclusiva al rispetto della vita privata e approdi nel contesto del "mercato dei dati", anche l'autodeterminazione individuale al trattamento rischia di risentirne [26]: il consenso quale emblema di una forma di protezione forte da ingerenze altrui nella sfera personale immateriale, diviene uno strumento di controllo delle elaborazioni "predittive", compiute su quei dati dalle *data companies*. Da qui, si è osservato che il consenso quale condizione di ammissibilità al trattamento costituisce una mera adesione, che pur consapevole e informata, non è dissimile da quella di consumatori e utenti dinanzi al contratto standardizzato [27], e che, divenendo consenso "negoziale", la volontà personale nella logica dello scambio animata dalla digitalizzazione abbia mutato ruolo, unitamente alle forme del controllo sulla circolazione a fini commerciali dei dati personali [28].

Nella direzione di una disillusione verso uno strumento di selezione di ciò che la persona è disposta a cedere, ha contribuito l'impressione che la prestazione del consenso, sottesa all'accesso a un servizio dal contenuto digitale, non sia una scelta del tutto libera, se dominata dalla logica dello scambio, tanto da risultare condizionata alla controprestazione offerta dal professionista. E, più radicalmente, si è poi sostenuto che la trasposizione del consenso dell'interessato nel perimetro del contratto [29] abbia avviato l'autodeterminazione del titolare del dato a una parabola discendente [30] o che, il consenso dinanzi alle tecniche di elaborazione dei dati sia svuotato di contenuti, tanto da divenire un "mito", nei confronti del quale già nel 1973 Stefano Rodotà ammoniva [31].

Eppure, dietro l'adozione di opzioni ermeneutiche che del consenso al trattamento testimoniano una perduta centralità, si annida il rischio di mistificare una fuga dalla regola di autodeterminazione, posta a «formale baluardo della tutela dell'individuo» [32], e di mortificare la primazia del consenso pur laddove essa non venga nel piano delle regole scalfita. La rilevanza del consenso e della specificità delle finalità del trattamento, come definite nel momento iniziale della raccolta dei dati, permangono infatti quali elementi fondanti del-

---

[25] Sulla quale cfr. P. PERLINGIERI, *La personalità umana nell'ordinamento giuridico*, Camerino-Napoli, 1972, *passim.*

[26] Si veda R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contr. e impr.*, 2020, 760 ss. Cfr. A. DE FRANCESCHI, *La circolazione dei dati tra privacy e contratto*, Napoli, 2017, 12.

[27] C. CAMARDI, *Mercato delle informazioni e privacy. Riflessioni generali sulla l. n. 675/1996*, in *Europa dir. priv.*, 1998, 1057; S. RODOTÀ, *Tecnologia e diritti*, Bologna, 1995, 41 s.

[28] C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, cit., 59.

[29] Sulla quale, già in passato, F.G. VITERBO, *Protezione dei dati personali e autonomia negoziale*, cit., *passim*, relativamente alla possibilità di rendere i dati personali oggetto di accordi di natura negoziale, non già quale forma di negozialità dei dati personali, ma quale espressione di negozialità dell'*an* e del *quomodo* del trattamento dei dati (*ivi*, 110 ss.) e relativamente ai possibili modelli di negoziazione delle regole di trattamento (*ivi*, 247 ss.).

[30] Si vedano C. BASUNTI, *La (perduta) centralità del consenso*, cit., 860 ss.; V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *I dati personali nel diritto europeo*, cit., 38 ss.; I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale*, in *Annali. Università degli studi Suor Orsola Benincasa*, Napoli, 2018, 7 ss. (nonché in *Osserv. dir. civ. comm.*, 2018, 1, 67 ss.); F. STASSI, *Consenso dell'interessato e dati personali al tempo dei big data*, in *Riv. dir. ec. trasp. amb.*, XIX, 2021, 105 ss.; M.G. STANZIONE, *La protezione dei dati personali tra «consumerizzazione» della privacy e principio di accountability*, in *Comparazione dir. civ.*, 2022, 1, 1 ss.

[31] S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, 45 ss.

[32] C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, cit., 59.

la regolazione europea. Ed è semmai fuori dallo spettro dei trattamenti ordinari, nel contesto di trattamenti massivi dei *big data*, che si percepisce una sostanziale perdita di controllo sul dato ad opera dell'interessato, determinata da fattori estranei alla regolazione normativa [33].

Tra questi campeggia la riduzione della soglia di attenzione dell'interessato, dinanzi a reiterate richieste di consenso da parte delle *data companies* con conseguenze in ordine alla capacità cognitiva dell'informativa, tali da compromettere l'integrità del processo decisionale che precede il consenso al trattamento. Dinanzi al fenomeno dei *big data* l'utente d'altronde non ha a che fare con dati dotati di immediata attitudine comunicativa e pertanto egli comprende meno di quanto quei dati possano dire di sé a professionisti del settore. Una disattenta prestazione del consenso è allora frequentemente incoraggiata dalla scarsa dimestichezza con i servizi della società dell'informazione o dalla naturale inaccessibilità del navigatore medio alla comprensione di meccanismi dall'elevato livello di complessità o sofisticazione o, ancora, dalla sensazione che la circolazione in forma aggregata di una vasta mole di dati riesca a maggiorare i vantaggi dei servizi offerti rispetto ai rischi di nocumento alla propria persona.

Contribuisce inoltre a ridurre il controllo dell'interessato sulla circolazione del dato la difficoltà di revocabilità del consenso, possibilità predisposta dal legislatore europeo ma talvolta svuotata 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 considerare il caso in cui essa sia inibita dall'avere ceduto contrattualmente il dato personale).

Ancora, a dismettere la centralità del consenso per i trattamenti massivi concorre un processo di depersonalizzazione del dato, funzionale a ridurre i rischi di vulnerabilità dell'utente "profilabile", attraverso l'impiego di alcuni strumenti di sicurezza che ne impediscono la profilazione: tecniche di *anonimizzazione* (come la *generalizzazione* o la *randomizzazione*) e di *pseudonomizzazione* (come la *crittografia* o la *tokenizzazione*) [34]. Con le prime si priva il dato personale in modo definitivo della sua capacità identificativa, ad esempio generando distorsioni o alterazioni tali da rendere il dato personale non riconducibile all'utente e, di conseguenza, avulso dal qualificarsi dato personale conformemente alla regolazione europea, la cui applicazione sarebbe dunque preclusa. Eppure queste tecniche non risolvono il rischio di una re-identificazione dell'utente ad opera dei *data players* [35]. Diversamente, 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 disciplina europea [36]. Ebbene, anche la diffusione dei riferiti strumenti di alterazione della capacità identificativa del dato potrebbe costituire un sintomo della marginalizzazione in questo ambito del ruolo del consenso dell'utente.

Proprio nel tentativo di far fronte alle complessità del fenomeno dei *big data*, sprovviste di specifica regolazione giuridica, il 30 maggio 2017, l'Autorità *antitrust*, l'Autorità garante delle comunicazioni e quella per la protezione dei dati personali hanno avviato, di concerto, un'indagine conoscitiva per esaminare le implica-

---

[33] A.C. NAZZARO, *L'utilizzo dei Big data e i problemi di tutela della persona*, cit., 1239 ss.

[34] F. STASSI, *Consenso dell'interessato e dati personali al tempo dei big data*, cit., 123.

[35] Ammonisce dai rischi di una reidentificazione P. OHM, *Broken Promisese of Privacy: Responding to the Surprising Failure of Anonymization*, in *UCLA Law Review 57*, 2010, 1, 1701 ss.

[36] L'art. 4, n. 5, *GDPR* 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».

zioni dello sviluppo del fenomeno dei *big data* sulle regolazioni della protezione dei dati personali, delle comunicazioni elettroniche e della tutela del consumatore [37].

Eppure è legittimo dubitare che le dinamiche di cui si è riferito rilancino nella dimensione del diritto generale la riferita neutralizzazione del consenso al trattamento: il titolare del dato in effetti non smarrisce la sua originaria signoria fuori dallo spettro di interazione dei *big data*, e dunque laddove la sua autodeterminazione sia più esposta all'evoluzione tecnologica. A pensar diversamente, si negherebbe la centralità del consenso rispetto ai trattamenti ordinari, con il rischio di accelerare quei processi di mercificazione del dato personale che assottigliano il potere determinativo dell'interessato. La trattazione che segue si propone, quindi, di verificare il perdurante rilievo dell'autodeterminazione individuale nel quadro dell'attuale regolazione normativa sulla circolazione dei dati personali e di riflettere le specificità dei trattamenti dotati di carattere massivo e pervasivo, più difficilmente riconducibili a una prospettiva esclusivamente individuale.

2. – Com'è noto, il principale referente normativo della circolazione del dato personale, a livello europeo, è costituito dal reg. 2016/679/UE, "*General Data Protection Regulation*" (di seguito "*GDPR*") [38] e alla dir. 2016/680/UE, attuata con il d.lgs. 10-8-2018 n. 101, che ha modificato il d.lgs. 30 giugno 2003 n. 196, codice della *privacy*. Occorre aggiungere che la contrattualizzazione del dato personale è stata di recente suggellata dalla positivizzazione dello schema di cessione del dato, *ex* art. 3, par. 1, della dir. 2019/770/UE, "*Digital Content Digital Services*" (*DCDS*) [39], attuata con il d.lgs. 4 novembre 2021 n. 173, che ha inserito il Capo I-bis "Dei contratti di fornitura di contenuto digitale e di servizi digitali" (artt. 135-*octies*-135-*vicies ter*) al titolo III della parte IV del codice di consumo.

Ma il tentativo di uniformare le discipline nazionali dei paesi dell'Unione Europea [40], indotto dalla globalità dei fenomeni riferiti in premessa, approda con il *GDPR* al momento terminale di un processo di regola-

[37] L'indagine conoscitiva, dopo l'audizione 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 informazione ai grandi operatori digitali, si è conclusa con la delibera 458/19/CONS, adottata nel novembre 2019 dall'Autorità garante delle comunicazioni.

[38] Dell'abbondante bibliografia in commento al *GDPR* si segnalano le opere collettanee: AA.VV., *La nuova disciplina europea della Privacy*, a cura di S. Sica, V. D'Antonio, G.M. Riccio, Padova, 2016; AA.VV., *I dati personali nel diritto europeo*, cit.; AA.VV., *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel regolamento UE 2016/679*, a cura di L. Califano, C. Colapietro, Napoli, 2017; AA.VV., *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da G. Finocchiaro, Bologna, 2017; AA.VV., *Regolare le tecnologie: il Reg. UE 2016/679 e la protezione dei dati personali*, a cura di A. Mantalero, G. Finocchiaro, Pisa, 2018; AA.VV., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, a cura di R. Panetta, Milano, 2019; AA.VV., *Privacy digitale: riservatezza e protezione dei dati personali, tra GDPR e nuovo Codice privacy*, a cura di E. Tosi, Milano, 2019; AA.VV., *Persona e mercato dei dati: riflessioni sul GDPR*, a cura di N. Zorzi Galgano, Padova-Milano, 2019; AA.VV., *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, a cura di G. Finocchiaro, Bologna, 2019; A. Barba, S. Pagliantini, *Delle persone. Leggi collegate*, II, in *Comm. cod. civ.*, diretto da E. Gabrielli, Milano, 2019; nonché AA.VV., *GDPR tra novità e discontinuità*, cit., 2777 ss.

[39] Si rinvia in proposito al par. 7 del presente lavoro.

[40] Si segnala oltretutto che di recente non sono mancati rilevanti tentativi analoghi di regolazione in altri ordinamenti, come la legge federale russa n. 152-FZ o il canadese "*Personal Information Protection and Electonic Document Act*" (*PIPEDA*) o il "*California Consumer Privacy Act*" (*CCPA*). Quest'ultima è una legge statale della California, adottata nel 2018 e in vigore dall'1 gennaio 2020, sulla protezione dei dati personali circolanti per finalità di consumo, che si applica a tutte le società a scopo di lucro che nel mondo: *a*) vendono le informazioni personali di oltre 50000 utenti all'anno, persone o *devices*, residenti in California; *b*) hanno un fatturato annuo lordo superiore a 25 milioni di dollari o derivano più del 50 per cento del loro fatturato annuale dalla vendita delle informazioni personali dei residenti californiani (sez. 1798.140 del corpo normativo). Si tratta di una disciplina del modo in cui le imprese che rispondono alle riferite soglie sono autorizzate a trattare le informazioni personali dei cittadini residenti in California.

zione che è stato avviato con le due direttive: *a*) dir. 1995/46/CE [41], cd. direttiva "madre", recepita dal legislatore nazionale con la l. 31 dicembre 1996, n. 675; *b*) e dir. 2002/58/CE, c.d. "*ePrivacy*", attuata in Italia con il codice della *privacy* del 2003 [42], oltretutto coevo al recepimento italiano della dir. 2000/31/CE, ad opera del d.lgs. 9 aprile 2003, n. 70, sul tema contiguo del commercio elettronico.

L'armonizzazione affidata alle due direttive, mantenendo la logica di protezione di un diritto della personalità [43], quale la riservatezza, si proponeva di contrastare eventuali interferenze altrui con la sfera personale [44], rese più frequenti dalla necessità di assicurare le libertà fondamentali, in linea con il Trattato di Maastricht, e segnatamente la libera circolazione dei dati nel contesto intracomunitario. Si è osservato che in questa fase di disciplina europea è mancata una ricostruzione calibrata in termini patrimonialistici [45] e che poi, con il *GDPR,* il 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» [46]. Eppure si potrebbe obiettare che già allora la prospettiva di tutela fosse «quella del titolare del trattamento (…) cioè quella degli interessi del titolare» [47]. Nel tentativo di farsi carico delle istanze sottese alla previgente disciplina europea, il consenso della persona interessata era definito dall'art. 2, lett. *h*, dir. 46/95, «manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali siano oggetto di un trattamento», una definizione questa già indulgente verso la considerazione del dato nel contesto di un'attività economica [48]. Ma, pur trattandosi di una disciplina che già si muoveva oltre l'orizzonte della tutela della persona, per dar conto degli obiettivi istituzionali dell'Unione, l'esigenza di fare i conti con la portata esponenziale dei flussi informativi di dati personali, nel contesto dell'economia contemporanea, era rimasta sullo sfondo.

La contestualità di opposti interessi si consolida nel *GDPR*. Per un verso viene riproposta una definizione di consenso sostanzialmente conforme all'art. 4, n. 11: «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». E, per altro verso, nel complesso si osserva nel Regolamento una certa «enfasi sul momento circolatorio dei dati personali, rispetto alla sottolineatura delle implicazioni personalistiche del

---

[41] L'art. 29 dir. 46/95 ha istituito il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali (*WP29*), composto dal Garante europeo della *privacy*, da un rappresentante per ciascuna autorità nazionale e da un rappresentante della Commissione, gruppo di lavoro poi sostituito dal Comitato europeo per la protezione dei dati ("*European Data Protection Board*", *EDPB*).

[42] Sul consenso nel codice della *privacy*, tra i tanti, si vedano 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.; e F.G. VITERBO, *Protezione dei dati personali e autonomia negoziale*, cit., 181 ss.

[43] L'art. 1, par. 1, dir. 46/95 prevedeva infatti che «gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali». Sul punto, si veda l'analisi di 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*, cit., spec. 43 ss.

[44] In proposito G.B. FERRI, *Privacy, libertà di stampa e dintorni*, in *Europa dir. priv.*, 1998, 137 ss.; C. CASTRONOVO, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, *ivi*, 653 ss.; V. RICCIUTO, *Il trattamento dei dati relativi allo svolgimento di attività economiche*, *ivi*, 685 ss.; C. CAMARDI, *Mercato delle informazioni e privacy*, cit., 1049 ss.

[45] V. RICCIUTO, *La patrimonializzazione dei dati personali*, cit., 27.

[46] F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2017, 2, 375.

[47] C. CASTRONOVO, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, cit., 664.

[48] In tal senso l'art. 1, par. 2, dir. 46/95 già prevedeva che «gli Stati membri non possono restringere o vietare la libera circolazione dei dati personali tra Stati membri, per motivi connessi alla tutela garantita a norma del paragrafo 1», ossia «la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata».

dato personale» [49] e «un diverso bilanciamento degli interessi, che opera in favore della circolazione e con una retrocessione della tutela personalistica» [50].

Certamente, il legislatore europeo già da tempo premeva per favorire la circolazione in massa dei dati e per realizzare una piena integrazione economica e sociale attraverso la creazione del mercato unico [51]. Ma nel *GDPR*, pur riproponendo le istanze di tutela della persona, matura una consapevolezza che il dato personale, come si è osservato in precedenza, presenti una componente economica e si riveli merce di scambio di un sistema "dato-centrico", ponendosi, d'altronde, al crocevia delle tendenze riferite in premessa: tanto l'emersione della centralità del dato personale, al contempo oggetto di un diritto della personalità e, per taluni, già bene giuridico; quanto la declinazione "digitale" dell'identità personale, sottesa all'attenzione normativa al concetto di profilazione. In questa direzione un indice del venir meno dell'esclusività della dimensione non patrimoniale si reperisce nell'espunzione dal recepimento italiano del *GDPR* di ogni riferimento ai concetti di "identità personale" e di "dignità umana", sui quali erano state edificate le prime costruzioni normative sulla tutela dei dati personali [52].

Nel contesto normativo del *GDPR* la protezione dei dati nel tempo è divenuta d'altronde un obiettivo da perseguire sin dalla progettazione del trattamento (c.d. "*privacy by design*"), e anche mediante impostazioni predefinite (c.d. "*privacy by default*"), che rimangono tali, in assenza di una modifica da parte dell'utente (ad es. la possibilità che i *post* di un *social network* siano visualizzati non soltanto dalla cerchia dei contatti dell'utente). Ne discende che la regolazione europea dei dati personali è intrisa di quella logica binaria che mischia la deferenza verso l'autodeterminazione informativa con il "*risk based approach*" [53], caricandosi di quella funzione "conformativa" dell'operazione economica nel cui oggetto figura il dato [54].

E l'idea che lo sfruttamento dei dati personali possa compiersi anche a scapito della protezione dell'individuo, come in altre forme di regolazione [55], non è dunque estranea al *GDPR* [56]: lo si evince ad esempio nella verifica della compatibilità delle diverse finalità, pur lecite, delle successive operazioni sui dati rispetto alla finalità originaria del trattamento ai sensi dell'art. 5, par. 1, lett. *b*; o, dinanzi al trattamento necessario *ex* art. 21, par. 1 (come per l'esecuzione di un compito di interesse pubblico), nell'espressa indicazione dei mo-

---

[49] F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, cit., 375; conforme anche G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, 1, 1 ss.

[50] A. IULIANI, *Note minime in tema di trattamento dei dati personali*, in *Europa dir. priv.*, 2018, 1, 302.

[51] F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Padova, 2018, 195 ss.; C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, cit., 37 ss., spec. 38, che osserva come il *GDPR* costituisca la sintesi di un conflitto, «il diritto alla protezione dei dati personali *versus* l'esigenza di circolazione dei dati», che si formalizza dal punto di vista normativo, tanto a livello unitario quanto nazionale.

[52] S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, 583 ss.; anche se già allora si presagiva la breve fortuna dell'esclusività del fondamento personalistico della tutela della *privacy* (S. SIMITIS, *Il contesto politico e giuridico della tutela della privacy*, *ivi*, 575 ss.).

[53] In tal senso depongono le sezioni II (Sicurezza dei dati personali), artt. 32-34, e la sezione III (Valutazione d'impatto sulla protezione dei dati e consultazione preventiva), artt. 35-36, *GDPR*, che vincolano il titolare del trattamento all'analisi del rischio e alla verifica dell'impatto sulla protezione dei dati dell'interessato, disposizioni che pure sono funzionali alla tutela della persona che sta dietro i dati. In proposito G. GIANNONE CODIGLIONE, *Risk-based approach e trattamento dei dati personali*, in *La nuova disciplina europea della Privacy*, cit., 58; C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, cit., 33.

[54] Si veda R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, cit., 769 ss.; C. PERLINGIERI, *Data as the Object of a Contract and Contract Epistemology*, in *The Italian Law Journal*, 2019, 2, 624 ss.

[55] Il "*California Consumer Privacy Act*" (*CCPA*) prevede, ad esempio, la generica possibilità di raccogliere, utilizzare e vendere i dati da parte delle imprese, con la sola eccezione della vendita di dati di consumatori minorenni, per cui si deve avere l'esplicito consenso (*opt-in*) del minore di 16 anni o del genitore o tutore del minore di 12 anni.

[56] Come osserva F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, cit., 380.

tivi di opposizione dell'interessato per la sua situazione particolare (e sempreché non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato); né è più richiesta l'autorizzazione del Garante per il trattamento di categorie particolari di dati sensibili (come quelli relativi alla salute), bastando il consenso dell'interessato, in seguito all'abrogazione dell'art. 26 cod. privacy. Ne consegue che la protezione del dato non costituisce più una prerogativa assoluta dell'interessato [57], con la conseguenza di appannare la sacralità della *privacy* quale diritto fondamentale e inviolabile, indiscussa piuttosto nei trattati europei [58].

Completa il quadro d'insieme la constatazione che nel mercato dei dati personali i principali attori sono divenuti i *data players* dell'economia digitale. Ne discende una ulteriore accentuazione della prospettiva del titolare da parte del *GDPR*, ossia di colui che individua mezzi e finalità del trattamento (art. 4, n. 7, *GDPR*), ma anche di quella del soggetto "responsabile", ossia di colui che tratta i dati per conto del titolare (art. 4, n. 8, *GDPR*), in luogo dell'originaria esclusività della autodeterminazione del titolare del dato. Conseguentemente, lo sviluppo della regolazione dei modelli organizzativi imprenditoriali e degli adempimenti in capo ai titolari e ai responsabili ridimensiona nel *GDPR* un'eventuale fuga dalla tutela della persona.

Il rapporto tra utenti e utilizzatori è dunque sfociato nella combinazione tra due polarità simmetriche ed opposte: da un lato la libertà di circolazione del dato, che si riflette sul trattamento, e dall'altro la responsabilità nel trattamento, che la regolazione europea sintetizza, nella consapevolezza che tutto ciò che aumenta la prima si risolve in un incremento della seconda [59].

La libertà nel trattamento opera uno spostamento del punto di equilibrio tra il diritto dell'interessato e l'interesse legittimo – se così possa qualificarsi [60] – del titolare del trattamento in senso indubbiamente più propizio al secondo. Semmai l'interessato mantiene il c.d. diritto alla portabilità dei dati (art. 20 *GDPR*), con il quale è legittimato a pretendere dal titolare del trattamento la messa a disposizione dei propri dati personali, 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. Sul punto va rilevato che non sempre risulta agevole assicurare una effettiva portabilità delle informazioni da un operatore a un altro della società dell'informazione, magari perché all'utente non conviene migrare ad altro operatore, essendo impossibile riprodurre la stessa capacità relazionale con il nuovo operatore. L'"effetto rete" costituirebbe un fattore contrario alla migrazione da un *social network* a un altro, disincentivata dal rischio per l'utente di c.d. *lock-in* sociale [61].

Di contro, la responsabilizzazione del titolare del trattamento opera quale contrappeso a una circolazione di dati personali "libera", prevedendo il principio di *accountability* [62], cioè il principio che impone di

---

[57] Lo prevede espressamente il considerando n. 4 *GDPR*: «il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali in ossequio al principio di proporzionalità».

[58] Così A. IULIANI, *Note minime in tema di trattamento dei dati personali*, cit., 306 ss.; F. PIRAINO, *I "diritti dell'interessato" nel Regolamento generale sulla protezione di dati personali*, cit., 2799.

[59] La nota correlazione evoca l'aforisma «*Tout ce qui augmente la liberté augmente la responsabilité*» (V. HUGO, *Actes et paroles*, *Depuis l'Exil*, Paris, 1876, 40).

[60] Come espressamente previsto dinanzi al trattamento necessario *ex* art. 6, lett. *f*, *GDPR*. Cfr. A. IULIANI, *Note minime in tema di trattamento dei dati personali*, cit., 302, che osserva che il rapporto soggetto-bene non si coglie nello schema della prevalenza prefigurata proprio del diritto soggettivo, ma «nella dimensione della sua effettività e attualità».

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

[62] In proposito R. CATERINA, *Novità e discontinuità nel Regolamento generale sulla protezione dei dati personali*, in *GDPR tra*

rendere conto delle proprie condotte rispetto a un determinato obiettivo, con il conseguente effetto di responsabilizzazione, che obbliga tutti i responsabili del trattamento ad 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* [63]. Qualora poi il trattamento dei dati personali sia basato sul consenso, il *GDPR* riserva al titolare del trattamento sia la scelta della modalità di acquisizione del consenso sia la conseguente dimostrazione di averlo acquisito. L'art. 7 *GDPR* prevede infatti che qualora il trattamento dei dati personali sia basato sul consenso «il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso».

L'esposta linea di lettura, che nel *GDPR* percepisce lo sforzo di cogliere il fenomeno di crescente patrimonializzazione dei dati personali, pur in continuità con la disciplina previgente, non deve tuttavia intendersi come un'operazione interpretativa volta a svilire gli spazi di tutela della persona, che la regolazione europea contiene. Il legislatore europeo non sarebbe dunque artefice di una sterilizzazione della protezione della persona, messa semmai a dura prova dall'evoluzione della quale sono protagonisti i dati personali.

3. – La mediazione del diritto del titolare dei dati personali con le dinamiche osservate si coglie all'esame del rilievo normativo del consenso, che – in continuità con l'art. 7 della direttiva "madre" [64] – il *GDPR* all'art. 6 mantiene quale prima base giuridica del trattamento. La manifestazione di consenso ad opera dell'interessato basterebbe ad escludere una valutazione di necessità del trattamento prevista invece in tutti gli altri casi. L'art. 6 *GDPR* ammette sì che il consenso al trattamento dei propri dati personali per una o più specifiche finalità sia una delle condizioni di liceità, e che oltretutto – a un criterio "topografico" – si rivela la principale, ma non mancano ipotesi di trattamento che prescindono dall'autodeterminazione dell'interessato [65], come laddove il trattamento sia necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi e a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali

novità e discontinuità, 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». Di recente M.G. STANZIONE, *La protezione dei dati personali tra «consumerizzazione» della privacy e principio di accountability*, cit., 1 ss.

[63] Il parere n. 3/2010 reso dal Gruppo di lavoro *WP29* sulla protezione dei dati personali aveva già reso necessario che il titolare del trattamento per attuare i principi di protezione dei dati adottasse misure appropriate ed efficaci e che queste fossero dimostrate all'interessato che ne avesse fatto richiesta. Un secondo livello di responsabilizzazione, poi, si riscontrava nei sistemi di responsabilità di natura volontaria, eccedenti le norme di legge minime. Si veda G. FINOCCHIARO, *Il principio di accountability*, in *GDPR tra novità e discontinuità*, cit., 2778 ss.

[64] Si noti che nella direttiva "madre" la centralità del consenso quale prima base giuridica del trattamento all'art. 7 trova rispondenza nella priorità del consenso all'art. 8, par. 2, per consentire trattamenti vietati dal legislatore dello Stato membro, dinanzi a categorie particolari di trattamenti, come quelli di dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale, salvo in questa evenienza la legislazione dello Stato membro abbia escluso che il consenso della persona interessata non sia sufficiente per derogare al divieto di trattamento.

[65] Il trattamento, ai sensi dell'art. 6 *GDPR*, prescinde dal consenso dell'interessato, nei casi in cui 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 (lett. *b*); il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (lett. *c*); il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica (lett. *d*); 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 (lett. *e*); 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 (lett. *f*).

dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore (art. 6, par. 1, lett. *f*, *GDPR*) [66]. La disposizione, dando luogo a un complesso bilanciamento, postula una comparazione al suo interno affidata al titolare del trattamento, considerata espressione di una visione "titolare-centrica" nella gestione delle interferenze lesive negli spazi di autodeterminazione rimessi all'interessato [67]. La necessità del trattamento, di contro, non attiene solo alla sfera dell'*an*, essendo necessario verificare il grado di incidenza del titolare del trattamento (che riguarda la sfera del *quomodo*). La compressione del diritto alla protezione dei dati personali è giustificata solo all'esito del positivo superamento del vaglio di proporzionalità dell'incidenza, che costituisce oltretutto misura e criterio di valutazione dell'*accountability* del titolare [68].

Si osserva allora sì che, al fianco del consenso, il parametro della necessità del trattamento entri a comporre la stessa nozione di liceità del trattamento e che, in luogo del presupposto di legittimazione principale, ulteriori basi giuridiche, al passo con i tempi e a seconda delle circostanze, possono rivelarsi più appropriate del consenso a fondare il trattamento [69]. Ma, per ciò solo e stante la continuità con la disciplina previgente, sarebbe difficile trarre un'inequivoca indicazione circa una perdita di centralità del consenso rispetto ad altre basi giuridiche del trattamento. E d'altronde quel diffuso pessimismo circa la sorte del consenso [70], difficil-

---

[66] Al minore che abbia compiuto sedici anni, l'art. 8 *GDPR* riconosce il potere di esprimere il consenso al trattamento dei dati personali per quanto riguarda l'offerta diretta di servizi della società dell'informazione, riservando ai singoli Stati membri la facoltà di fissare un'età differente, ma non inferiore ai tredici anni. Il legislatore italiano ha quindi inserito nel codice *privacy* l'art. 2-*quinquies*, che fissa tale limite nei quattordici anni. In proposito, R. SENIGAGLIA, *Minore età e contratto. Contributo alla teoria della capacità*, Torino, 2020, 75 ss., che riflette sulla capacità di concludere i relativi contratti per il minore quattordicenne, che si autodetermina al trattamento dei propri dati personali, a fronte del carattere anche patrimoniale del consenso all'utilizzo del dato. L'interdipendenza tra la dimensione personale e quella patrimoniale porta l'A. a ritenere che anche il minore contrente, legittimato a dare il consenso al trattamento dei dati, sia abilitato ad esprimere il consenso contrattuale allo scambio tra dati e fornitura dei servizi digitali. Si tratterebbe infatti di «un unico atto oggettivamente complesso» al quale concorrono due atti di volontà inseriti nel medesimo senso funzionale e quindi interdipendenti, «tanto che parrebbe assurdo riconoscere la capacità rispetto ad uno di essi e disconoscerla rispetto all'altro».

[67] D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *GDPR tra novità e discontinuità*, cit., 2784; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, 2016, 153.

[68] Il titolare del trattamento deve d'altronde provvedere a indicare, ai sensi dell'art. 24 *GDPR*, misure tecniche e organizzative adeguate alla natura, alla finalità, al contesto, all'ambito di applicazione del trattamento.

[69] D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, cit., 2784; F. STASSI, *Consenso dell'interessato e dati personali al tempo dei big data*, cit., 110; C. BASUNTI, *La (perduta) centralità del consenso*, cit., 873. Cfr. M.G. STANZIONE, *La protezione dei dati personali tra «consumerizzazione» della privacy e principio di accountability*, cit., 1 ss.

[70] In proposito, F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, cit., 384 s., secondo il quale «con una salutare professione di realismo andrebbe riconosciuto che il consenso è soltanto uno dei presupposti di liceità e del trattamento e, al limite, base giuridica applicabile di default nei casi dubbi»; A. IULIANI, *Note minime in tema di trattamento dei dati personali*, cit., 306 ss., che afferma che «l'evoluzione descritta incide in maniera determinante sul consenso che non rappresenta più il *prius* per la circolazione, ma diventa una delle condizioni successive, neppure la prevalente»; D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, cit., 2784, che osserva che «ammesso che il consenso al trattamento abbia mai avuto un periodo di reale fasto, sono sempre più frequenti oggi i richiami al suo declino, alla sua recessione, alla sua parabola discendente»; V. CARBONE, *Il consenso, anzi i consensi, nel trattamento informatico dei dati personali*, in *Danno e resp.*, 1998, 1, 30, per il quale «affidare al solo consenso la tutela della *privacy* comporterebbe il riconoscimento di una sconfitta per l'ordinamento»; F. STASSI, *Consenso dell'interessato e dati personali al tempo dei big data*, cit., 110, che sostiene che «il consenso riveste dunque una posizione decentrata, perché nella logica del Regolamento tutte le basi giuridiche hanno un'analoga valenza»; analogamente A.C. NAZZARO, *L'utilizzo dei Big data e i problemi di tutela della persona*, cit., 1239 ss.; M.G. STANZIONE, *La protezione dei dati personali tra «consumerizzazione» della privacy e principio di accountability*, cit., 1 ss.; C. BASUNTI, *La (perduta) centralità del consenso*, cit., 873, per il quale «il consenso ai fini del trattamento dei dati personali non garantisce sempre l'effettività del controllo del singolo, esso si sostanzia spesso in una mera adesione che, nonostante sia di natura diversa rispetto alla manifestazione di volontà adesiva al contratto contenente condizioni generali *ex* artt. 1341 e 1342 c.c., è tuttavia paragonabile a quella che i consumatori comunemente rilasciano

mente potrebbe valere a negare che il consenso rappresenti una condizione diversa dalle altre, quanto meno perché rende il trattamento in presenza di una o più finalità conforme all'intento dello stesso interessato.

Nella prospettiva di assicurare la legittimità del trattamento sollecitando l'autodeterminazione dell'interessato andrebbe letto anche l'obbligo, che, anteriormente ad esso, l'art. 12 *GDPR* pone a carico del titolare del trattamento, di fornire agli interessati l'informativa relativa alle finalità e alle modalità, che deve essere resa agevolmente accessibile e intelligibile per l'interessato, conformemente al considerando n. 39 *GDPR*. Il consenso deve infatti prestarsi in relazione alle finalità e alle modalità palesate dal titolare del trattamento (consenso c.d. specifico). La finalità, pertanto, costituisce una forma di perimetrazione del consenso, tanto che la volontà dell'interessato si estende a tutte le attività di trattamento svolte per la stessa o le stesse finalità, mentre qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste, come previsto dal considerando n. 32 *GDPR*.

Ma non è escluso che il trattamento per una finalità diversa da quella per la quale i dati personali sono stati inizialmente raccolti, pur non basato sul consenso dell'interessato o su un atto legislativo (dell'Unione o degli Stati membri) che costituisca una misura necessaria e proporzionata per la salvaguardia degli obiettivi di cui all'art. 23, par. 1, *GDPR*, possa essere compatibile con la finalità che ha mosso la raccolta. In questo caso l'art. 6, par. 4, *GDPR* – innovando rispetto alla direttiva "madre" – consente che il titolare del trattamento verifichi la compatibilità della finalità diversa con quella o quelle originarie, alla luce di alcuni criteri («*a*) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; *b*) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; *c*) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9 oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10; *d*) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; *e*) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione»). La formulazione tortuosa della previsione rivela il tentativo di supplire all'assenza di base giuridica per il trattamento preordinato a finalità diverse, rendendo allora sufficiente, a un giudizio di compatibilità della finalità diversa, la base giuridica del trattamento per cui i dati sono stati inizialmente raccolti. Anche in questo caso, come nell'art. 6, par. 1, lett. *f*, va in scena la prospettiva "titolare-centrica", che mette in gioco una correzione del trattamento sguarnito del consenso preordinato alle finalità individuate. L'art. 6, par. 4, *GDPR*, quindi, costituisce una delle più nitide indicazioni nel senso di quella marginalizzazione del consenso, sia pur da riferire al trattamento per finalità diverse.

Eppure, uno sguardo all'architettura del regolamento indurrebbe a non drammatizzare il tentativo, in atto, di neutralizzazione del consenso dell'interessato. In questa direzione può osservarsi che, per il trattamento di categorie particolari di dati personali, l'art. 9, par. 2, lett. *a*, *GDPR* ha accantonato il sistema autorizzatorio – in parte svuotato di significato dalla proliferazione delle autorizzazioni generali previste dall'art. 40 cod. privacy – optando piuttosto per la sufficienza del consenso dell'interessato, senza lasciare alcuno spazio per l'introduzione di requisiti ulteriori. E, ancora, che le condizioni di validità del consenso – preteso dall'art. 7 *GDPR*, nelle modalità di manifestazione, ''esplicito'' e ''inequivocabile'' – confermano la centralità del consenso nella necessità dell'accertamento della sua liceità: il medesimo consenso può consentire sì la conclusione del contratto, ma al tempo stesso non rivelarsi dotato dei requisiti di validità per il trattamento dei dati personali. Per il caso in cui il trattamento dei dati sia svolto con il consenso dell'interessato nel contesto

per la sottoscrizione di contratti di massa uniformi». E, sotto quest'aspetto, cfr. C. CAMARDI, *Mercato delle informazioni e privacy*, cit., 1057; D. POLETTI, *Tecnologia e diritti*, cit., 41 s.

di una dichiarazione scritta che riguarda anche altre questioni, il titolare del trattamento, sul quale grava l'onere di dimostrare che l'interessato lo abbia manifestato, deve presentare la richiesta di consenso, «in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro» (art. 7, par. 2, *GDPR*). Conseguentemente, il consenso richiesto dal titolare del trattamento – a differenza di quanto previsto nella prima legge italiana in materia di protezione di dati personali – non può che essere veicolato da "un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale" (considerando n. 32 *GDPR*). Risponde alla regola posta di consenso "espresso" sia la manifestazione esplicita di volontà sia quella implicita, sottesa a un comportamento attivo, in modo da escludere ogni dubbio che con la propria azione l'interessato abbia voluto comunicare il proprio consenso (c.d. inequivocità del consenso [71], tale per cui non sarebbe dunque sufficiente un consenso tacito). Il legislatore europeo avalla dunque un modello 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, così come statuito dai noti arresti della Corte di giustizia [72] (sui quali più avanti si tornerà).

Fin qui l'esteriorizzazione del consenso, nella quale tuttavia non si esaurisce la validità del consenso, che, come si evince dal considerando n. 32 *GDPR*, attiene altresì alla sua formazione, richiedendosi che esso sia prestato liberamente e che sia revocabile. In proposito l'art. 7, par. 4, *GDPR* prevede che deporrebbe in senso contrario a una libera determinazione dell'interessato 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 necessario all'esecuzione di tale contratto [73]. Quanto alla revocabilità, l'art. 7, par. 3, *GDPR* – innovando rispetto alla direttiva "madre" – accorda all'interessato il diritto di revocare in qualsiasi momento il proprio consenso, senza che con ciò si pregiudichi la liceità del trattamento basata sul consenso prima della revoca. E infatti, in difformità delle condizioni previste dal *GDPR* [74], il consenso ottenuto non sarebbe vincolante.

Orbene, tutta questa attenzione riservata dal legislatore alle condizioni alle quali il consenso sia validamente prestato, sintomatiche della centralità che il consenso ancora riveste sul piano normativo, inducono a non sopravvalutare tentativi di dismissione del consenso, come quelli maturati in seno all'art. 6, par. 4, *GDPR*, per suggerirne piuttosto una riduzione teleologica, che ne ridimensioni la portata dirompente in linea con l'esigenza di conformazione dei modelli di circolazione dei dati alle concrete esigenze di tutela della persona [75].

---

[71] A riprova dell'inequivocità del consenso depone lo stesso considerando n. 32 *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».

[72] Tra i quali spiccano le pronunce Corte eur. giust. 1-10-2019 C-673/17, *Planet 49*, e Corte eur. giust. 11-11-2020 C-61/19, *Orange Romania*.

[73] Relativamente a un'operazione di *tying* antecedente l'entrata in vigore del *GDPR*, si veda Cass. 2-7-2018 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 *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. Sul punto F. STASSI, *Consenso dell'interessato e dati personali al tempo dei big data*, cit., 112, nt. 15.

[74] Condizioni peculiari sono previste per il consenso dei minori in relazione ai servizi della società dell'informazione. L'art. 8 *GDPR* prevede che 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 il consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

[75] Cfr. F.G. VITERBO, *Protezione dei dati personali e autonomia negoziale*, cit., *passim*.

4. – Passando poi a verificare quale sia la natura del consenso richiesto quale base giuridica del trattamento, è condivisibile che la riferita cornice normativa fornisca indicazioni circa una visione negoziale del consenso dell'utente: essa avrebbe soppiantato letture più tradizionali del consenso, retaggio della riconduzione del diritto alla riservatezza del dato personale a un diritto indisponibile.

Alla tesi della natura non negoziale [76], che qualifica il consenso come manifestazione di volontà con funzione scriminante di un'attività altrimenti illecita, dunque autorizzazione alla stregua del consenso di cui all'art. 50 c.p., si contrappone una qualificazione negoziale dello stesso [77]. Quest'ultima obietta all'opposto orientamento che una qualificazione di condizione di liceità del trattamento (ad esempio per superare il divieto di trattamento di dati sensibili, biometrici e genetici *ex* art. 9, par. 2, lett. *a*, *GDPR*) non sarebbe di per sé incompatibile con la tesi negoziale, che non mortifica il ruolo dell'autodeterminazione, anzi lo valorizza, mostrandosi più consona alle tendenze osservate in premessa, e dunque alla luce della "libera circolazione" dei dati [78]. La lettura "negoziale" del consenso, scettica nel ritenere l'attività sui dati personali di natura illecita [79], condivide l'idea che il consenso abbia funzione dispositiva dei dati personali, non soltanto assunti a dignità di bene, in quanto elementi che orbitano nella sfera del soggetto, ma addirittura cedibili e trasferibili, quali merci di scambio per la fornitura di un servizio.

L'opzione ermeneutica, nel cogliere le tendenze in atto, ricorre alla nozione di "appartenenza" all'interessato dei dati personali, «senza che sia necessario stabilire se il titolo sia proprietario o meno» [80]. L'estensione della logica proprietaria ai dati personali [81] d'altronde non andrebbe esente da alcune condivisibili obiezioni. Si osserva che il regime di circolazione del dato personale è connotato dalla persistenza di un incisivo potere di controllo sulle modalità di utilizzazione della risorsa, che travalica il primo atto di disposizione del diritto [82], tanto che la volontà dell'interessato al trattamento dei dati personali non potrebbe produrre il medesimo effetto traslativo di cui all'art. 1376 c.c. Non verrebbe in rilievo quindi un consenso traslativo, in quanto l'interessato non potrebbe dismettere la titolarità del dato personale. Gli effetti dell'assenso all'altrui ingerenza nella propria sfera giuridica, semmai, consistono in obblighi di comportamento sia in capo all'interessato, sia in capo al titolare del trattamento [83].

---

[76] In tal senso, tra i tanti, G. MIRABELLI, *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *Dir. inf.*, 1993, 313 ss.; 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.; nonché ID., *Commento all'art. 23*, *La protezione dei dati personali. Commentario al d.lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, a cura di C.M. BIANCA, F.D. BUSNELLI, I, Padova, 2007, 543 ss., che qualifica il consenso al trattamento dei dati personali come un elemento della fattispecie legale che farebbe venire meno l'antigiuridicità dell'attività relativa ai dati.

[77] In favore di una lettura "negoziale" del consenso 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. Cfr. S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, cit., 1026 ss.; F. CAGGIA, *Libertà ed espressione del consenso*, in *I dati personali nel diritto europeo*, cit., 269; A. FICI, E. PELLECCHIA, *Il consenso al trattamento*, in *Diritto alla riservatezza e circolazione dei dati personali*, a cura di R. PARDOLESI, Milano, 2003, 469 ss.

[78] F. STASSI, *Consenso dell'interessato e dati personali al tempo dei big data*, cit., 115.

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

[80] G. OPPO, *Sul consenso dell'interessato*, cit., 124; in proposito anche C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, cit., 74 ss.

[81] G. ALPA, *La proprietà dei dati personali*, in *Persona e mercato dei dati: riflessioni sul GDPR*, cit., 9 ss.; cfr. F.G. VITERBO, *Protezione dei dati personali e autonomia negoziale*, cit., 99.

[82] Così G. RESTA, *Autonomia privata e diritti della personalità*, cit., 118; A.C. NAZZARO, *L'utilizzo dei Big data e i problemi di tutela della persona*, cit., 1239 ss.

[83] S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Riv. dir. civ.*, 2001, 633

Ora si può anche non essere d'accordo sull'applicazione di regole proprietarie al "dato-informazione", per coglierne l'attitudine rappresentativa della persona, l'idoneità a identificarla [84], ma appare incontestabile come la lettura negoziale rifletta meglio l'autodeterminazione individuale all'atto di adesione al contratto per la prestazione del servizio. Un'adesione, si è riferito, in definitiva analoga a quella di utenti e consumatori al cospetto della predisposizione di contratti di massa uniformi. L'accesso al *web* costituisce «un comportamento concludente attraverso il quale l'interessato manifesta la propria disponibilità affinché altri raccolgano ed elaborino le proprie informazioni» [85]. Si aggiunga che l'inclusione dei dati personali nel perimetro dell'oggetto contrattuale, fungendo sostanzialmente da controprestazione, assume ampio risalto, specie dinanzi a quelle operazioni contrattuali che – frequentemente di recente – riguardano trattamenti massivi di dati personali. Come vicenda negoziale il consenso non soltanto può dunque vestire i panni sia di una manifestazione di volontà pura e semplice, atto di determinazione non piegato alla logica dello scambio, ma può giustificarsi in vista della (contro)prestazione di un servizio.

Da ultimo, la tendenza in atto alla patrimonializzazione degli attributi immateriali della persona e, segnatamente, allo sfruttamento ad opera del titolare [86] depone inequivocabilmente per una qualificazione negoziale del consenso. Eppure l'adesione alla lettura negoziale potrebbe costituire occasione per promuovere un riavvicinamento alla sponda personalistica, un'opportunità di recupero del momento di controllo ad opera della persona dell'atto di autonomia privata in funzione della salvaguardia degli stessi valori che risultano coinvolti [87].

In questo senso, ci si pone sulla stessa traiettoria delle riflessioni espresse alla fine del secolo scorso da 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 (…)», perché 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 in parte, dimostrano quindi che c'è una scelta dell'interessato che definisce l'area della protezione» [88].

5. – Si è accennato che la definizione dell'art. 4, n. 11, *GDPR* prevede che il consenso sia specifico: il che equivale a dire che la sua prestazione debba circoscriversi alle attività su dati, alle finalità del trattamento e a quegli stessi dati per il quale esso è stato rilasciato. Da qui la possibilità per l'interessato di prestare il proprio consenso: *a*) per una o più attività, senza rilasciarlo per altre; *b*) o nell'ambito di taluni trattamenti, per una o più finalità, escludendone altre; *c*) o ancora, pur ammettendo un trattamento per una o più finalità per alcuni dati, non autorizzarlo per altri. Il consenso dell'interessato si ritaglia quindi sul trat-

---

ss.

[84] Cfr. G. ALPA, *La proprietà dei dati personali*, cit., 9 ss.; C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, cit., 45.

[85] Così F. CAGGIA, *Libertà ed espressione del consenso*, cit., 255; V. RICCIUTO, *La patrimonializzazione dei dati personali*, cit., 38 ss.

[86] Tra i più, si veda S. THOBANI, *Diritti della personalità e contratto*, cit., 94 ss.

[87] Sul bilanciamento tra diritto alla *privacy* e circolazione dei dati personali, F. PIRAINO, *I "diritti dell'interessato" nel Regolamento generale sulla protezione di dati personali*, cit., 2797 ss.

[88] Così S. RODOTÀ, *Conclusioni*, in *Trattamento dei dati personali e tutela della persona*, cit., 308, come ricordato anche da V. RICCIUTO, *La patrimonializzazione dei dati personali*, cit., 29 s., e da F. STASSI, *Consenso dell'interessato e dati personali al tempo dei big data*, cit., 116.

tamento, calibrando il potere di signoria della persona sul concreto atto di incidenza delle *data companies* sul dato personale.

Questa "granularità" si traduce per il titolare del trattamento in una moltiplicazione delle richieste di consenso da trasmettere all'utente, in relazione alle diverse attività, finalità e dati per i quali si intende ottenere la manifestazione di volontà. Si pensi all'utilizzo dei dati per finalità di *marketing*: in questo caso occorre una richiesta distinta per autorizzare l'invio di aggiornamenti sulle attività e sulla pubblicazione di *post* sul *web* o di annunci pubblicitari o di attività a scopo promozionale e di inviti ad eventi.

Di recente, le Linee guida 4 maggio 2020, n. 5, adottate dallo *European Data Protection Board* (*EDPB*), aggiornando le disposizioni del 10 aprile 2018, tentano un recupero del rilievo della volontà dell'utente dinanzi all'utilizzo dei dati nella rete, regolando l'accettazione dei *cookie* di un sito *web* da parte dell'utente, ossia di tutte quelle informazioni immesse sul *browser* degli utenti [89], in navigazione sul *web*. Anche i dati raccolti attraverso i *cookie*, non ascrivibili in prima battuta a informazioni personali (così come i dati analitici anonimizzati), possono considerarsi tali in via mediata, per deduzione o in combinazione con altri dati, poiché forniscono in ultima istanza identificazione univoca dell'utente. L'utente, allora, prima di accedere al sito *web*, deve autorizzarne l'uso [90], analogamente ad ogni altra tecnologia di tracciamento di navigazione, mediante una volontà positiva e frazionabile.

Sotto il primo profilo, il modello dell'*opt-in*, ricavabile dall'indicazione legislativa europea di un consenso formalizzato in una condotta positiva che ne attesti l'inequivocabilità, induce inoltre a escludere che possa valere come consenso un'opzione preselezionata da deselezionare (*opt-out*). Mancherebbe un contegno dell'utente, tale da qualificare come manifestazione di volontà. In proposito, la Corte di Lussemburgo, sul caso *Planet 49* [91], ha statuito che dall'utilizzo di una casella preselezionata non è desumibile che l'utente di un sito *web* abbia inequivocabilmente accettato l'installazione dei *cookie*. Dinanzi a una casella che contenga già il *flag* di accettazione, il navigatore potrebbe non avere letto la didascalia posta a fianco della casella o addirittura potrebbe non averla notata.

In questi casi si rivelano inadatte a costituire consenso dell'interessato sia le attività di scorrimento di una pagina *web* per rimuovere il *banner* comparso all'accesso (c.d. *scrolling*), sia quelle attività minime di 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 quel consenso esplicito e inequivocabile, sotteso al modello dell'*opt-in*.

Per altro verso, poi, la "granularità" del consenso consentirebbe di manifestare la volontà dell'interessato in riferimento soltanto ad alcuni tracciamenti e non ad altri: le menzionate Linee guida impediscono i c.d. *cookie walls*, 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 troverebbe davanti a un "muro" che, con palese alterazione

---

[89] I *cookie* costituiscono *file* di testo che il fornitore di un sito *internet* invia all'utente che lo abbia visitato, per registrare dati e impostazioni di personalizzazione relativi al servizio che il sito offre. La loro funzione è dunque di riconoscere e tracciare l'attività dell'utente, o per consentirgli un migliore accesso, riconoscendo l'utente stesso in caso di una nuova navigazione (*cookie* c.d. "tecnici") – come nel caso dell'impostazione di una lingua predefinita su un sito *web*, scelta memorizzata in vista degli accessi successivi – o per creargli un *identikit* attraverso l'utilizzo di algoritmi di calcolo (*cookie* c.d. "di profilazione"). In proposito G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione*, Torino, 2016, 230 ss.; nonché A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, cit., 55.

[90] In proposito G. MARINO, Internet *e tutela dei dati personali: il consenso ai cookie*, in questa *Rivista*, 2020, 2, 398 ss.

[91] Corte eur. giust. 1 ottobre 2019, cit., 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*, 19-2-2020, e da A. REINALTER, S. VALE, *Cookie e consenso dell'utente*, in *Giur. it*., 2020, 1, 79 ss.

della sua libertà di autodeterminazione, condizionerebbe la fruizione del servizio alla preventiva e generalizzata manifestazione di consenso al trattamento dei suoi dati.

Una diversa impostazione rispetto ai *cookie* è offerta dal "*California Consumer Privacy Act*" (*CCPA*), che – salvo per i minori di 16 anni [92] – non basa l'utilizzo dei *cookie* sul consenso dell'interessato, prevedendo piuttosto la generica possibilità di raccolta delle informazioni personali, purché il *web tracker* venga posto a conoscenza di quali dati siano da raccogliere e con quali parti siano condivisi. Laddove poi il consumatore abbia venduto queste informazioni, il perimetro dell'obbligo informativo include l'indicazione delle categorie di dati che vengono condivise con terzi per scopi commerciali, in modo da potere consentire al consumatore l'esercizio del diritto di *opt-out* alla vendita, mediante la predisposizione sulla *homepage* del sito *web* dell'impresa di un apposito *link* obbligatorio con la dicitura "*Do not sell my personal information*".

Si segnala, tuttavia, che di questi tempi la specificità, attributo del consenso che si pone quale anticamera della granularità, risente di non poche difficoltà dinanzi all'incapacità, nel contesto dei *big data*, di individuare un uso specifico al momento della raccolta dei dati, per poterlo comunicare all'utente [93], anche a causa della terzietà del soggetto "estrattore" rispetto all'operatore che potrebbe beneficiarne per finalità commerciali.

Per ovviare all'inconveniente di un consenso "non specifico", occorre muovere dalla presa d'atto dell'indeterminatezza dell'uso specifico al momento della raccolta dei dati. Nei casi in cui sia impossibile predeterminare la finalità del trattamento, dunque ostacolandosi il reperimento della base giuridica principale del trattamento, potrebbe allora sostituirsi la specificità del consenso che l'utente manifesta in relazione alla finalità del trattamento con l'imposizione al titolare del trattamento di una valutazione comparativa dei diversi interessi in campo, tra i quali il rischio che si infligge alla sua sfera personale [94]. Un'operazione in fondo non dissimile da quella prevista dall'art. 6, par. 4, *GDPR*, per i trattamenti piegati a finalità diverse da quella per la quale è stato prestato il consenso. In questo caso, tuttavia, si impone l'accortezza di non indulgere a un eccessivo favore verso gli interessi delle imprese: la valutazione dovrebbe quindi tradursi nel vaglio preventivo 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 invece 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 dell'accertamento preventivo da parte dell'autorità di controllo [95], onde evitare che l'esito perda di obiettività. Una siffatta proposta, pur non incarnando il modello dell'*opt-in* avallato dalle Corti, richiede egualmente che sia lasciata all'utente la facoltà di esercitare un diritto di *opt-out*, per ritirare il consenso manifestato all'esito della valutazione preventiva [96].

6. – Una riprova della centralità del consenso dell'interessato, a scapito di deriva interpretativa della rego-

[92] Per i quali, il *CCPA* stabilisce per l'impresa l'obbligo di fornire i *banner* per l'*opt-in* necessario per il consenso dei minori ovvero del loro rappresentante laddove si tratti di minore infradodicenne.

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

[94] 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.

[95] Così A. MANTALERO, *La privacy all'epoca dei Big data*, cit., 1193.

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

lazione europea che ne colga il suo declino si coglie, di recente, nelle pronunce della Corte di giustizia. In continuità con la sentenza *Planet 49*, il giudice europeo ha suffragato il modello dell'*opt-in* con la sentenza dell'11-11-2020 sul caso *Orange Romania* [97], pronunciandosi sul rinvio pregiudiziale presentato dal Tribunale di Bucarest relativamente alla valida prestazione del consenso degli interessati e alla dimostrazione della sua esistenza nei contratti di fornitura di servizi di telefonia conclusi tra costoro e la società rumena.

La questione interpretativa era originata dalla presenza nei contratti di una clausola secondo cui l'interessato era stato informato e aveva validamente manifestato il proprio consenso alla raccolta e alla conservazione di una copia del documento di identità ai fini dell'identificazione, nel caso in cui la casella relativa a una siffatta clausola fosse stata selezionata dal titolare del trattamento prima della sottoscrizione. A ben vedere la *Orange Romania* non subordinava la fornitura del servizio 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. Eppure della possibilità di stipulare il contratto anche in caso di rifiuto al trattamento l'interessato non era adeguatamente informato, in modo da ingenerare il dubbio circa una sua autodeterminazione effettivamente libera e informata [98].

La Corte afferma che la prova di un valido consenso dell'interessato spetti al titolare del trattamento e che costui nel caso di specie non ha dimostrato né una manifestazione di volontà inequivoca, né libera e informata.

Sotto il primo profilo non basta la preselezione di una casella "di spunta" per provare un consenso inequivoco del titolare del trattamento. La circostanza che detti clienti abbiano sottoscritto i contratti contenenti la casella selezionata non consente, di per sé, di dimostrare un siffatto consenso, in assenza di indicazioni che confermino che tale clausola sia stata effettivamente letta e assimilata.

Conseguentemente, sotto ulteriore profilo, la Corte disapprova che, in combinato con l'automatismo di un consenso al trattamento, un contegno esplicito dell'interessato sia piuttosto richiesto per opporsi alla raccolta e alla conservazione dei dati, tramite l'aggravio della compilazione di un modulo supplementare, tale da incidere indebitamente sulla libera scelta di opporsi. Pare dunque che la Corte veicoli l'idea di una doppia sottoscrizione, sottostante alla necessità di una determinazione espressa sia per il contratto di abbonamento sia per il consenso al trattamento dei dati, quasi ad evocare la regola del consenso espresso alle prestazioni supplementari *ex* art. 65 cod. cons. [99].

La necessità di assicurare una scelta libera e consapevole del cliente è *ratio decidendi* che tuttavia nella pronuncia fonde le ragioni della trasparenza consumeristica con quelle della protezione dei dati personali, sottese alle questioni sorte sugli attributi del consenso. Questa sovrapposizione ingenera una confusione non

---

[97] Corte eur. giust. 11 novembre 2020, cit., 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.*, 2021, 1, 247 ss.

[98] Si veda in proposito il punto 45 della sentenza della Corte: «dalle indicazioni contenute nella menzionata domanda risulta che, sebbene detti contratti contengano una clausola secondo la quale i clienti interessati sono stati informati e hanno manifestato il loro consenso alla conservazione di una copia del loro documento d'identità a fini identificativi, la casella relativa a tale clausola era già stata selezionata dagli agenti di vendita dell'*Orange Romania* prima che tali clienti procedessero alla firma recante accettazione di tutte le clausole contrattuali, ossia tanto di detta clausola quanto di altre clausole non connesse alla protezione dei dati. In detta domanda viene inoltre indicato che, senza che i contratti di cui al procedimento principale lo precisino, l'*Orange Romania* accettava di stipulare tali contratti con clienti che rifiutassero di prestare il loro consenso alla conservazione di una copia del loro documento d'identità, esigendo al contempo, in tal caso, che detti clienti firmassero un modulo specifico che attestasse il loro rifiuto».

[99] Come prevede l'art. 65 cod. cons., il professionista, in assenza del consenso espresso, laddove lo abbia dedotto «utilizzando opzioni prestabilite che il consumatore deve rifiutare per evitare il pagamento supplementare, il consumatore ha diritto al rimborso di tale pagamento».

consona a dotare di specificità il tema del consenso al trattamento dei dati personali, le cui cautele nel reperimento dei suoi attributi, sottostando alla disciplina del *GDPR*, non hanno alcuna esclusiva giustificazione in funzione pro-concorrenziale.

L'autodeterminazione al trattamento si rivela tanto libera quanto più la si renda informata, dovendosi consentire all'interessato di individuare agevolmente le conseguenze del consenso prestato, in modo da assicurare che la sua determinazione avvenga consapevolmente. E qui la Corte disapprova la mancata informazione dell'interessato sulla natura "condizionata" o "opzionale" del consenso richiesto. Non è escluso che se le parti avessero compreso il carattere opzionale del consenso al trattamento si sarebbero determinate negativamente alla raccolta e conservazione dei dati personali. La Corte di giustizia pertanto dichiara l'insussistenza di un'effettiva volontà dell'interessato laddove le clausole contrattuali possano indurre l'interessato in errore circa la possibilità di stipulare il contratto anche in caso di mancanza del consenso al trattamento dei dati.

Nella pronuncia una eventuale "forzatura" del consenso ad opera del professionista è dunque stigmatizzata a prescindere dal carattere condizionato dell'autodeterminazione dell'interessato: l'assenza di un'adeguata informazione ad opera del titolare del trattamento circa la non necessità è in grado di procurare una supposizione di necessità, che rende forzato il consenso. E il testo contrattuale deve evitare forzature del consenso, sottese alla subordinazione del servizio alla prestazione di esso o alla induzione in errore dell'interessato, tendendo piuttosto ad assicurare nell'interessato il convincimento che il suo rifiuto non comprometta la prestazione del servizio ad opera dell'altro contraente [100]. Ove ciò non avvenisse, il consenso sarebbe viziato e si potrebbero attivare i rimedi per il *vulnus* inferto al proprio diritto.

Nel ragionamento della Corte, dunque, il consenso non è forzato se l'interessato è in grado di compiere una scelta libera, perché non vincolata da una preselezione, e informata, perché consapevole del carattere condizionato o meno della prestazione. Eppure, nel caso del rilascio del consenso come prestazione "condizionale" all'ottenimento di un bene o un servizio, strettamente connessi al trattamento dei propri dati, l'informazione dell'interessato non sempre evita una "forzatura" del consenso, per così dire più fisiologica: l'interessato si ritrova costretto a determinarsi positivamente al trattamento sul modello "*take it or leave it*" [101]. In questa evenienza, il consenso è posto quale antecedente necessario a conseguire (e a conservare) la posizione giuridica oggetto dell'attribuzione voluta dall'utente, e pertanto la sua prestazione non costituisce una scelta autonoma dall'acquisto del bene e del servizio, né è prevista una attribuzione economica per l'eventuale cessione del dato personale, nonostante spesso l'accesso al servizio o l'acquisto del bene abbiano un valore inferiore rispetto al "prezzo" del consenso [102]. L'evenienza rivela allora l'inidoneità del libero rilascio della volontà dell'utente a costituire l'oggetto di un vincolo obbligatorio e il contratto per suo conto rischierebbe di risultare viziato per conflitto con norme imperative che prescrivono l'incoercibilità del consenso al trattamento [103]. Eppure il conflitto con il prototipo normativo del consenso "libero", come si è osservato [104], è sopito dal buon esito della aspettativa collegata allo scambio.

---

[100] C. ANGIOLINI, *A proposito del caso Orange Romania*, cit., 264.

[101] Sul punto C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, cit., 102 ss.; V. RICCIUTO, *La patrimonializzazione dei dati personali*, cit., 38 ss.

[102] La locuzione richiama il sintagma adoperato da Cass., 16 maggio 2008, n. 12433, sullo sfruttamento dell'immagine altrui, in *Foro it.*, 2008, I, c. 3215, con nota di T.M. UBERTAZZI, *Dubbi sulla revocabilità del consenso all'utilizzazione dell'immagine*; e *Giust. civ.*, 2009, I, 706 ss., con nota di D. SIMEOLI, *Il «prezzo del consenso» quale criterio di liquidazione del danno patrimoniale derivante dall'illecita pubblicazione dell'immagine altrui.*

[103] G. RESTA, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il Regolamento UE 2016/679*, in *Annuario del contratto. 2018*, 2019, 127 ss., spec. 145.

[104] C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, cit., 104.

Situazioni di autodeterminazione forzata si riscontrano sia "in occasione" o "in vista" di beni e servizi (ad es. il diritto all'accesso e all'uso di un *social network*, la possibilità di utilizzare un motore di ricerca), sia "in ragione" dell'ottenimento di beni e servizi (ad 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) [105]. Il consenso al trattamento può quindi rivelarsi strumentale allo svolgimento della fase precontrattuale o all'esecuzione di un contratto con fornitori di servizi in posizione dominante [106]. 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. Ma lo scambio risulta giustificato perché si tratta di servizi che sono interamente o prevalentemente finanziati dalla pubblicità, che si avvalgono del consenso quale unica controprestazione.

7. – Ulteriori riflessioni sulla relazione tra consenso al trattamento e contratto hanno origine, com'è noto, dall'accennata formalizzazione, in luogo di uno scambio informale, di un accordo di cessione del dato personale, ad opera della dir. 2019/770/UE, *Digital Content and Service Directive*, che ha disciplinato alcuni aspetti dei contratti di fornitura e di servizi digitali. La direttiva, all'art. 3, par. 1, nell'individuare l'ambito applicativo, prevede che la cessione di un dato personale possa costituire, mediante un'operazione complessa, controprestazione per la fornitura di contenuti o servizi digitali da parte di un operatore economico [107]. 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 [108] (talvolta con la possibilità di accedere con un sovrapprezzo ad un pacchetto *premium*) o, qualora sia previsto un corrispettivo, con la possibilità di beneficiare di uno sconto a fronte della cessione dei dati personali.

Per la verità 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 0287/2015, 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 di una previsione che sottendesse una "mercificazione" del dato personale [109].

---

[105] F. STASSI, *Consenso dell'interessato e dati personali al tempo dei big data*, cit., 116.

[106] C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, cit., 102; V. RICCIUTO, *La patrimonializzazione dei dati personali*, cit., 38.

[107] L'art. 3, par. 1, dir. *DCDS* 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". Analogamente il considerando n. 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.

[108] C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, cit., 79 ss.

[109] L'*European Data Protection Board* aveva ritenuto infatti – alla nota 27 della opinione n. 4/2017 – 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*»). In proposito F. STASSI, *Consenso dell'interessato e dati personali al tempo dei big data*, cit., 118, nt. 34.

La nuova formulazione sovrappone una duplicità di piani consistente, da un lato, nel procedimento e nel consenso finalizzati alla conclusione del contratto di fornitura e, dall'altro, nel procedimento concernente la raccolta del consenso informato e l'esplicazione analitica delle finalità del trattamento, tanto che è parso venire in rilievo un doppio procedimento formale e un doppio consenso da parte dell'utente del servizio, sintomo di un collegamento tra due negozi [110]. Ma in ogni caso l'avere optato per una formulazione verbale più cauta non esclude che, pur in assenza di un corrispettivo monetario, in termini economici si compia uno scambio ("*non monetary transaction*"), sotto le spoglie di una fruizione del servizio a titolo gratuito, il cui controvalore economico consiste nell'atto unilaterale di autorizzazione al trattamento, accordato appunto in cambio di un servizio.

La direttiva provvede a congiungere la disciplina della protezione dei dati personali allo statuto consumeristico, in modo da implementare il potenziale rimediale a disposizione del consumatore-interessato [111] (come ad esempio dinanzi all'utilizzo da parte dell'operatore economico, nel contesto di una pratica commerciale scorretta, del materiale caricato dal consumatore, contenente dati personali, in vista dell'ottenimento di un servizio). Il novero dei rimedi contrattuali per la protezione dei dati personali del consumatore forniti all'operatore economico al momento della conclusione del contratto, o successivamente, si arricchisce ben oltre la tradizionale sponda della tutela individuale, mettendo in gioco una tutela di tipo amministrativo affidata all'Autorità Antitrust [112] (art. 66 cod. cons.) e quella collettiva (art. 140-*bis* cod. cons.), sulla quale incide altresì la dir. 2020/1828/UE, relativa alle azioni rappresentative per la tutela degli interessi collettivi dei consumatori [113]. E questo rafforzamento dei processi di *public enforcement* attesta il declino di una tutela della persona calibrata sull'attribuzione di poteri individuali da esercitarsi dinanzi alla giustizia ordinaria, per quella spersonalizzazione dei rapporti, figlia della standardizzazione dei rapporti *business to consumer* [114]. E la previsione ad opera del legislatore di altre forme di tutela, alternative a quella giurisdizionale ordinaria, persegue al contempo un effetto – che si osserva sul piano del fatto – deflattivo del contenzioso civile e sottrae la tutela dell'interessato da eventuali inefficienze che affliggono il sistema di giustizia civile.

Riportando la trattazione alla prospettiva del consenso dell'interessato, la formalizzazione del negozio di cessione del dato determina l'ingresso del consenso dell'interessato tra le dinamiche negoziali della 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 [115]. In questa veste il consenso diviene un atto di autodeterminazione "economica", la cui libera esplicazione è valore che preserva il mercato da fenomeni distorsivi che costituiscono, al contempo, lesione di interessi pubblici e di diritti fondamentali dell'individuo [116]. L'omessa

---

[110] C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali*, in *Giust. civ.*, 2019, 3, 499 ss., spec. 510 s.

[111] C. IRTI, *Consenso "negoziato" e circolazione dei dati personali* cit., 119 ss., spec. 170, che esamina le tutele dell'interessato-consumatore, che porta a un incremento di tutela rispetto alla tradizionale tutela privatistica individuale.

[112] Esemplari i provvedimenti AGCM dell'11 maggio 2017, nn. 26596 e 26597, nei confronti di *WhatsApp*, e del 29 novembre 2018, n. 27432, nei confronti di *Facebook*, relativi alla raccolta, allo scambio con terzi e all'utilizzo per finalità commerciali dei dati di navigazione degli utenti (inclusi i loro interessi *online*). Quest'ultimo provvedimento è stato poi impugnato nel procedimento dinanzi al Tar Lazio, conclusosi con le sentenze del 10 gennaio 2020, nn. 260 e 261, a loro volta confermate dal Consiglio di Stato con le sentenze del 29 marzo 2021, nn. 263 e 263-1.

[113] A. MANTALERO, *Personal Data for Decisional Purposes in the Age of Analytics: from an Individual to a Collective Dimension of Data Protection*, in *Comparative Law & Secur. Review 32*, 2016, 238 ss.

[114] C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, cit., 173. A proposito della perdita di centralità della tutela individuale del contraente debole A. PLAIA, *Profili evolutivi della tutela contrattuale*, in *Europa dir. priv.*, 2018, 92.

[115] F. STASSI, *Consenso dell'interessato e dati personali al tempo dei big data*, cit., 120.

[116] A. ZOPPINI, *Il diritto privato e i suoi confini*, Bologna, 2020, 177 ss.

comunicazione dell'utilizzo per fini commerciali dei dati forniti dall'utente durante l'accesso al servizio potrebbe impedire il libero esercizio dell'autodeterminazione economica dell'utente, generando una scelta disinformata a fronte di una pratica commerciale scorretta dell'operatore economico.

La sovrapposizione di istanze differenti (tutela della persona e tutela del mercato), giustificata nell'attuale società interconnessa dalla considerazione dei dati personali del consumatore quale risorsa destinata alla circolazione su scala globale, non può che portare alla complementarità della protezione della *privacy* rispetto a quella del consumatore, ponendosi (come già osservato sul caso *Orange Romania*) distinti obblighi informativi in relazione ai rispettivi fini di tutela [117]. Eppure il tentativo di coniugare persona e mercato non sempre fronteggia il rischio di trascurare la centralità della persona umana, «la cui tutela non può essere obliata dalla mera rilevanza economica delle proprie informazioni» [118].

8. – A seguito della sintetica ricognizione svolta si ha l'impressione che la trasposizione del consenso al trattamento nel contesto del mercato dei dati digitali non abbia determinato una parabola discendente del consenso dell'interessato, revocandone in dubbio l'originaria centralità. Semmai, interpretazioni della regolazione europea della *privacy* eccessivamente inclini a cogliere l'equivalenza di tutte le basi normative del trattamento incrementano la percezione di uno sradicamento dell'attività di trattamento dei dati personali dagli steccati del diritto della personalità, dando parvenza di un'incapacità di controllo dell'interessato, assai più di quanto il dato normativo non indichi. Né d'altronde la natura negoziale del consenso che di certo matura dalle dinamiche avviate implica necessariamente la presa d'atto che reificazione e – specialmente – mercificazione siano processi da ritenere, con una certa corrività o arrendevolezza, già compiuti o inarrestabili. Dinanzi al superamento dei rigidi steccati tra ambiti personali e patrimoniali il rischio di una distorsione interpretativa che intenda la regolazione europea dei dati personali come ormai distante dall'istanza di tutela della persona determinerebbe una non condivisibile sterilizzazione di quanto in ossequio alla sponda personalistica quella disciplina attualmente contiene. Quello sul dato personale è ancora un diritto della persona, nonostante la sua componente patrimoniale traduca talvolta il consenso dell'interessato in autodeterminazione economica dell'utente-consumatore.

La "tenuta" della primazia del consenso emerge d'altronde sia dal mantenimento di esso a elemento primo della liceità del trattamento, sia dall'enfasi normativa e giurisprudenziale accordata alla libertà, consapevolezza e inequivocità del consenso del titolare, che non può che portare a una riduzione teleologica del significato di altre disposizioni del *GDPR*, che – come l'art. 6, par. 4 – sembrano indurre a una dequotazione dell'autodeterminazione del titolare del dato. Ne consegue che osservare 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 le difficoltà applicative del principio di finalità sotteso al carattere specifico del consenso costituisce presa d'atto di un'apertura all'istanza di fruizione generalizzata delle informazioni nell'attuale contesto economico, senza con ciò tradursi in una complessiva erosione del consenso per i trattamenti ordinari.

Il rilievo del consenso dell'interessato nella circolazione dei dati personali oltretutto è testimoniato dalla prossima adozione di un regolamento *ePrivacy*, sulla tutela della vita privata nelle comunicazioni elettroniche, del quale il Consiglio d'Europa ha approvato nel febbraio 2021 una bozza, volta ad aumentare la prote-

[117] C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, cit., 177.
[118] C. BASUNTI, *La (perduta) centralità del consenso*, cit., 893.

zione degli utenti dalle minacce alla *privacy* che potrebbero derivare dall'utilizzo di strumenti di tracciamento (non solo *tracking cookie*, ma anche *spyware* o *web bugs* [119]). La bozza conferma il paradigma della scelta effettiva dell'utente, che potrà dirsi libera se non è pregiudicata la scelta tra un'offerta subordinata al consenso all'uso dei *cookie* per finalità aggiuntive (come quelle commerciali) e una scelta che ne prescinda pur essendo equivalente (considerando n. 2aaaa della bozza di proposta di regolamento). La bozza mantiene poi il "porto franco" dei servizi forniti in conformità della libertà di espressione e di informazione (ad es. giornali *on line*), al cui rilascio del consenso all'utilizzo di marcatori è subordinato il servizio. Eppure così facendo il recupero del controllo dell'utente sui suoi dati, sia pur quelli passivamente raccolti sui suoi terminali, avrebbe una ridotta operatività [120].

Come osservato in premessa, è semmai dinanzi ai trattamenti massivi di dati personali che la fuga dalla prospettiva dell'interessato pare più ampia di quanto non valga per i trattamenti individuali. Tanto che la professione ad opera del *GDPR* degli attributi del consenso e l'apporto ermeneutico fornito dalle corti in chiave di valorizzazione dell'autodeterminazione dell'interessato non garantiscono dai rischi insiti nei trattamenti su larga scala, nei quali allora il titolare del trattamento deve compiere una valutazione di impatto della protezione dei dati personali [121]. La circolazione dei dati nei casi di trattamenti abnormi aggirerebbe più frequentemente il consenso dell'interessato, che difficilmente sarebbe in grado di mostrarsi dotato dei suoi attributi (libero, esplicito, inequivocabile, specifico, etc.). Non tanto per la rarefazione della regola generale di prestazione del consenso, quanto più per l'ineffettività di una libera autodeterminazione dell'utente dinanzi all'evoluzione tecnologica dei dati, non dotati di una immediata portata informativa e sottoposti a trattamenti di consistente complessità. Qui il noto incedere dei flussi informativi nel mercato digitale ha posto in evidenza che il consenso, quale architrave dei poteri di controllo e intervento riconosciuti all'interessato sulle proprie informazioni, può essere "fisiologicamente" posto in discussione a causa dell'apporto di fenomeni che si dispiegano in tutto il loro spessore economico e che, pur conciliati con la tutela della persona, non risultano adeguatamente riflessi dall'attuale disciplina normativa. Si ha l'impressione che la regolazione europea della protezione dei dati personali – pur nella sintesi tra autodeterminazione informativa e approccio "*risk-based*" e pur con la consacrazione ad opera della corti del modello dell'*opt-in* – non riesca a fronteggiare appieno l'impatto sociale dei *big data* sulla *privacy* dell'interessato. La maggiore debolezza è costituita da un'inefficace previsione di meccanismi di selezione *ex ante* da parte dell'interessato [122]. Quali espedienti dunque per restituire al titolare del dato il suo potere di signoria in questi casi?

La necessità di caricare il consenso di una rinnovata funzione di meccanismo di partecipazione e di deci-

[119] Gli *spyware* costituiscono *software* che durante la navigazione in rete infettano segretamente il computer per monitorare e registrare l'attività dell'utente; i *web bugs* sono delle immagini invisibili, solitamente delle dimensioni di un *pixel* che vengono inserite all'interno di una pagina *web*, anche in questo caso per tracciare i contenuti dell'attività in rete dell'utente.

[120] Come osservato dall'*European Data Protection Board* (*EDPB*) nello *Statement* 2021, n. 3, adottato il 9 marzo 2021, sulla bozza di regolamento *ePrivacy*.

[121] Per i trattamenti che prevedono in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, l'art. 35, par. 3, *GDPR* prevede che il titolare del trattamento deve compiere una valutazione di impatto della protezione dei dati personali, quando il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche in caso di: «a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico».

[122] I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale. Iniziali spunti di riflessione*, in *Dir. merc. tecnol.*, 25 gennaio 2017, par. 5.

sione dell'interessato al trattamento dei dati personali è strada da tentare anche nel contesto dei trattamenti massivi. Ma, nella cornice dei *big data*, la sofisticata aggregazione insinua il dubbio che la soluzione politica di valorizzazione del consenso, come diritto di scelta che sia espressione di una libertà fondamentale, non riesca a soddisfare realmente l'aspirazione di coloro che intendano escludere il trattamento dei propri dati [123], avviando la ricerca di alternative di protezione «oltre una prospettiva esclusivamente individuale» [124].

In questo contesto l'immissione del dato in un vero e proprio mercato, che concorre allo sviluppo di un nuovo ordine economico, ha già prodotto alcuni tentativi di sostituzione della tutela individuale con quella collettiva e con quella privata sotto l'esercizio di poteri di *public enforcement*.

Ma il principale strumento di restituzione alla persona degli spazi a lei erosi è indubbiamente una più compiuta regolazione dei fenomeni osservati, attraverso l'ausilio della tecnica, e non esclusivamente nella direzione di un recupero della principale condizione di liceità del trattamento. Una tale operazione non va esente dal rilievo secondo cui l'illusione di una libera autodeterminazione non è poi tanto meno "paternalistica" dei meccanismi ispirati a regole di *default* ovvero ad altre strategie di "spinta gentile" (il cd. effetto "*nudge*") [125]. Si crede allora che interventi sostenuti dalla fiducia verso una scelta libera e consapevole dell'utente da soli non bastino, richiedendosi piuttosto la ricerca di nuove *regole di default* che beneficiano degli apporti dell'analisi comportamentale [126]. Una protezione effettiva dei dati personali non può dipendere da strategie incidenti sul comportamento dell'interessato, che non potrebbero apparire risolutive a fronte di una circolazione dai dati ormai irrimediabilmente nelle mani dei *data players*.

L'alternativa al consenso, ove esso sia aggirato, dovrebbe quindi passare attraverso un nuovo modello regolatorio, in grado di riflettere tutte le istanze in gioco. Il consenso, quale espressione di una *property rule*, potrebbe essere insufficiente oltre lo spettro dei trattamenti ordinari, mentre per i danni cagionati da trattamenti massivi, come per usi secondari, potrebbe rivelarsi più idoneo gravare di una *liability rule* chi incide sulla sfera della persona [127]. O ancora si potrebbe ovviare alla prestazione del consenso con un incremento delle regole procedurali, ampliative dell'*accountability* del titolare, che si traducono in norme tecniche interne ispirate a correttezza, alla minimizzazione del rischio di perdita di controllo da parte dell'utente e a valutazioni di sicurezza [128], ferme restando la permanenza in capo all'interessato del potere di inibire il trattamento e la risarcibilità dei danni cagionati dal trattamento.

La tendenza ad aumentare gli obblighi preventivi in vista di una responsabilizzazione del titolare del trattamento si riscontra, di recente, su sentieri contigui, in cui il legislatore europeo tenta l'elaborazione di disci-

---

[123] Il dubbio è condiviso da I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale*, cit. (*Annali*), 14, che si pone in prospettiva critica rispetto alle opzioni più di recente valorizzate (come il consenso al trattamento dei dati personali) dal legislatore europeo (il reg. *GDPR*) per verificarne i limiti, ovvero possibili scenari alternativi in prospettiva de *iure condendo*.

[124] C. ANGIOLINI, *A proposito del caso Orange Romania*, cit., 266.

[125] In proposito si veda il "paternalismo libertario" di R.H. THALER, C.R. SUNSTEIN, *Nudge. La spinta gentile. La nuova strategia per migliorare le nostre decisioni su denaro, salute, felicità*, trad. it. A. Oliveri, Milano, 2014; nonché C.R. SUNSTEIN, *Effetto nudge. La politica del paternalismo libertario*, trad. it. M. Barile, Milano, 2015; I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale*, cit. (*Annali*), 47.

[126] I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale*, cit. (*Annali*), 46 ss.

[127] I. COFONE, *The Dynamic Effect of Information Privacy Law*, in *Minnesota Journal of Law, Science & Technology*, 2017, 18, 2, 518 ss., spec. 542 ss.

[128] I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale*, cit. (Annali), 47. Cfr. M.G. STANZIONE, *La protezione dei dati personali tra «consumerizzazione» della privacy e principio di accountability*, cit., 1 ss.

pline "del rischio", che muovono dalla presa d'atto della rivoluzione digitale e si giustificano quale contrappeso della "socializzazione" dell'individuo: in questa direzione muove, com'è noto, la proposta di regolamento (COM(2020)825 del 15 dicembre 2020), nel quadro della Strategia per il mercato unico digitale in Europa (che annovera altresì l'armonizzazione delle discipline dei mercati digitali, c.d. *Digital Market Act*), per riformare gli obblighi e le responsabilità degli intermediari dei servizi digitali, mediante l'aggiornamento della dir. 2000/31/CE sul commercio elettronico, in vista di una disciplina organica dei servizi digitali (c.d. *Digital Services Act*).

Parallelamente a una valorizzazione del consenso dell'interessato, la regolazione della *privacy* dinanzi ai *big data* potrebbe destinarsi verso: *a*) l'incremento dei limiti al trattamento di taluni dati (come quelli a impatto discriminatorio); *b*) una graduazione della disciplina, conformemente al principio di proporzionalità previsto dal considerando n. 4 *GDPR*, in relazione al tipo di dati, oggetto di trattamento, sottoponibili a differente protezione in considerazione del diritto fondamentale che mettono in gioco (ad esempio, prevedendo la necessità del consenso per i dati c.d. "sensibili" e non per quelli non sensibili) [129]; *c*) lo sviluppo di tecniche più efficienti di spersonalizzazione del dato, capaci di ovviare ai rischi di una reidentificazione; *d*) e l'ampliamento degli strumenti di tutela (ad esempio, proponendo prestazioni sanzionatorie in capo ai soggetti responsabili o altre forme di reazione agli arricchimenti in capo all'autore dell'illecito, in quest'ultimo caso con la necessità di un'attenta valutazione dei criteri di determinazione del *quantum* restituibile o risarcibile) [130]. Muovere in questa direzione avrebbe il pregio di ridurre l'ineliminabile residuo di incapacità dei soli strumenti giuridici ad attutire «l'offensività strutturale dell'economia digitale sulla persona» [131].

[129] I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale*, cit. (Annali), 48, che osserva come «un modello regolatorio potrebbe avere in considerazione la possibilità di un superamento del requisito del consenso (o una sua interpretazione in senso restrittivo) con riguardo ai dati personali non sensibili, e ipotizzare una forma di controllo, sin dall'inizio, per l'interessato sui dati che rappresentano più strettamente la sfera dei diritti fondamentali, pur nella consapevolezza che esso non può rappresentare il principale baluardo della tutela. Questa distinzione, apprezzabile comunque nell'ottica di una più mirata protezione dei diritti della personalità, può rappresentare un ulteriore tassello per meglio definire il contenuto del diritto alla protezione dei dati personali, anche in ragione della verifica delle ipotesi in cui si possono determinare lesioni rilevanti della sfera privata, come visto in tema di danno da illecito trattamento».

[130] Si veda I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale*, cit., 49 s. Cfr. C. CAMARDI, *Note critiche in tema di danno da illecito trattamento dei dati personali*, in questa *Rivista*, 2020, 3, 786 ss., a proposito della relativizzazione della tutela aquiliana nel caso di illecito trattamento dei dati personali.

[131] C. CAMARDI, *Note critiche in tema di danno da illecito trattamento dei dati personali*, cit., 811, che osserva che «interessa solo argomentare come una corretta e appropriata impostazione dei rimedi contro l'offensività strutturale dell'economia digitale sulla persona non possa più sistemicamente essere regolata soltanto in chiave di responsabilità aquiliana, ma richieda l'utilizzazione di strumenti "altri" preventivi, di tipo macroeconomico se vogliamo, e non (soltanto) di diritto privato»; nonché C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, cit., 204.