

ILARIA AMELIA CAGGIANO

Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale

1. Dati personali e big data: portata del fenomeno e sua rilevanza nella società dell'informazione. Il mercato dei dati personali

Lo sviluppo esponenziale che caratterizza i processi tecnologici ha impresso nel torno degli ultimi due secoli profonde modificazioni ai rapporti sociali e, con essi, in senso adattativo o in funzione di limite, al diritto.

La tecnica, nel senso aristotelico di regola di attività, una volta informata dalla scienza, è stata in grado di caratterizzare in chiave deterministica il nostro tempo, sì da essere forza che travolge il tutto¹. In questo senso, una delle cifre unificanti ci sembra sia la centralità dell'informazione e della sua diffusione, in veste sempre meno di meta-narrazione, e sempre più diffusamente di bene di consumo e di scambio².

L'informazione, nell'era tecnologica, è il *dato*, memorizzato, raccolto massivamente, rapidamente trasmesso, tramite la rete Internet, e avente sempre più come oggetto l'individuo, scomposto, analizzato in frammenti di dati personali.

Appare chiaro che il flusso continuo di informazioni riguardanti l'individuo abbia modificato i comportamenti delle persone e quindi le libertà e i diritti a queste riferibili³. Avendo a mente tale variazione

1 In tal senso E. SEVERINO – N. IRTI, *Dialogo su diritto e tecnica*, Roma-Bari, Laterza, 2001.

2 J. F. LYOTARD, *La condition postmoderne*, Parigi, Minuit, 1979, trad. it. *La condizione postmoderna. Rapporto sul sapere*, Milano, Feltrinelli, 2014.

3 S. RODOTÀ, *Tecnologie e diritti*, Bologna, il Mulino, 1995; ID., *Intervista su Privacy e libertà*, a cura di P. Conti, Bari, Laterza, 2005. Parlano, efficacemente, di sistema "dato-centrico" A. MANTELERO, *The Future of Consumer Data Protection in the E.U. Rethinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics* (2014) 30 (6) *Computer Law & Security Rev.* 643 ff.; O. POLLICINO, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in «Diritto dell'informazione e dell'informatica», 2014, p. 569 ss.

può comprendersi (se non condividersi) il sorgere in capo al singolo di un distinto diritto alla protezione (e gestione) dei dati personali a lui riferibili, configurato in via autonoma rispetto alla sua identità o riservatezza⁴.

La raccolta e utilizzo massivo dei dati avviene per molteplici finalità (ad es. di sicurezza, scientifiche, di giustizia, commerciali) da parte di svariati soggetti privati o pubblici. Ciò non solo ha modificato le dinamiche, ovvero le potenzialità del controllo sociale, ma ha aperto a un nuovo mercato: quello dei dati personali.

Da un punto di vista fenomenico, la raccolta dei dati personali si realizza in vario modo: in occasione di prestazioni sanitarie; della conclusione di un contratto avente a oggetto beni o servizi e funzionalmente all'esecuzione delle prestazioni, ovvero all'ulteriore utilizzo da parte del titolare del trattamento a fini di vendita a terzi; da parte di *social network*, ove l'interazione digitale vede la rete sociale luogo di volontaria condivisione da parte degli utenti di contenuti che inevitabilmente contengono informazioni personali e che deliberatamente esprimono l'identità sociale dell'utente (dati relativi alla propria immagine, gusti, attraverso i tasti di apprezzamento o

4 L'idea che il singolo non solo abbia diritto a uno spazio di vita che non possa essere invaso da terzi (art. 7 Carta dei diritti fondamentali dell'UE), ma anche che i dati a lui riferibili siano protetti e rispetto al cui utilizzo egli abbia il potere di autodeterminarsi (si veda il consenso indicato come uno dei fondamenti legittimi del trattamento ai sensi dell'art. 8) rappresenta la lettura propria del diritto europeo che vede il diritto alla protezione dei dati come libertà fondamentale e quindi la tutela dei dati come formalizzazione dell'interesse della persona alla esplicazione della propria sfera personale. Sulla distinzione tra diritto alla riservatezza (o *privacy*) e alla protezione dei dati personali, da un punto di vista storico-sistematico e secondo il gergo comune (adottato anche dall'Autorità di settore), F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo regolamento europeo*, I, Torino, G. Giappichelli, 2106, p. 44 ss. Chiarisce C.M. BIANCA, *Diritto civile*, I, *La norma giuridica. I soggetti*, Milano, A. Giuffrè, 2002, p. 180 come nel linguaggio corrente *privacy*, riservatezza, protezione dei dati personali siano utilizzati in via alternativa. In termini più rigorosi, va rimarcata la distinzione tra un ampio di diritto alla riservatezza, nel quale confluiscono: il diritto alla riservatezza in senso tradizionale, come non divulgazione dei fatti della vita privata; una seconda accezione della riservatezza come intimità della sfera privata (*privacy*), che è l'accezione di riservatezza cui fa riferimento l'art. 2 cod. *privacy*; il diritto alla non ingerenza nei dati personali che è un'autonoma figura di diritto della personalità, a sua volta sancito a tutela di una pluralità di interessi essenziali della persona (vedi sempre art. 2 cod. *privacy*). Sul punto, per tutti, P. M. VECCHI, sub *art. 1*, in *La protezione dei dati personali. Commentario del Codice Civile*, a cura di C.M. Bianca e F. D. Busnelli, t. I, Padova, Cedam, 2007, p. 3 ss.

condivisione); da parte di motori di ricerca⁵.

Tali informazioni possono trasformarsi in profitto per l'ente privato attraverso la vendita a terze parti per finalità di *marketing*, pubblicitarie, di ricerca scientifica⁶. Lo sfruttamento commerciale delle informazioni personali come beni immateriali disponibili e negoziabili rappresenta la principale attività delle imprese che forniscono servizi digitali e elemento assolutamente dominante nelle economie moderne⁷. Il contenuto economico delle operazioni commerciali che implicano il trattamento di dati personali non può che essere tenuto in considerazione nell'opera di qualificazione e disciplina delle stesse⁸.

5 A. R. POPOLI, *Social Network e concreta protezione dei dati sensibili: luci ed ombre di una difficile convivenza*, in *Dir. info*, 2014, p. 981 ss. ove (testo successivo a nt. 40) «con la pressione di tasti di apprezzamento e di condivisione, si possono comunicare dati relativi all'origine razziale ed etnica, alle convinzioni religiose, filosofiche o di altro genere, alle opinioni politiche, [...] nonché dati idonei a rivelare lo stato di salute e la vita sessuale, ovvero dati sensibili...». Nelle dichiarazioni dei diritti e delle responsabilità di Facebook si legge che «l'utente concede a Facebook una licenza non esclusiva, trasferibile, che può essere concessa come sottolicenza, libera da *royalty* e valida in tutto il mondo, per l'utilizzo di qualsiasi contenuto IP pubblicato su Facebook o in connessione con Facebook».

6 «La raccolta, l'analisi, la conversione in statistiche di tutti i dati relativi dell'utente (inclusi i dati sensibili), anche per il tramite della licenza, rientrano nell'attività di *User Data Profiling*. [...] al fine di generare la segmentazione della propria utenza in gruppi omogenei di comportamento [...] realizzare *Behavioural Advertising* [...] nei *social network* sono gli utenti stessi a costruire un profilo di loro, che verrà utilizzato per la loro stessa profilazione», in A. R. POPOLI, *Social Network...*, cit. testo succ a nt. 84. In proposito, la informativa del social network Facebook chiarisce come la cd. licenza all'utilizzo dei dati venga utilizzata solo a fini di pubblicità redazionale e non per vendita a terze parti. Sebbene poi, in altro luogo, si dica espressamente: «Non condividiamo le tue informazioni personali (le informazioni personali comprendono nome o indirizzo e-mail che è possibile usare per contattarti o identificarti) con i partner pubblicitari, di misurazione o analisi, a meno che tu non ci conceda l'autorizzazione». Lo scenario come si vedrà *infra* al par. 4 è quanto mai complesso.

7 Si pensi solo al fatto che Google, diventata la seconda società al mondo per valore in Borsa, — con 522 miliardi di dollari di capitalizzazione, poco sotto i 587 miliardi di Apple, determini fatturati (di Alphabet, società cui fa capo) in continua crescita, soprattutto grazie i risultati ottenuti con la vendita degli spazi pubblicitari (fonti: www.corriere.it; http://www.corriere.it/economia/finanza_e_risparmio/16_aprile_26/wall-street-sorride-solo-gigante-google-2a13ebae-0b8f-11e6-a8d3-4c904844517f.shtml).

8 Con particolare riguardo a quelle fattispecie (social network, applicazioni, motori di ricerca) in cui il dato personale viene utilizzato come “merce di scambio” (frequente è in dottrina e nel linguaggio comune il riferimento ai dati personali come nuova moneta o nuovo petrolio), la pretesa “gratuità” di tali rapporti contrattuali nasconde una componente di tipo patrimoniale che caratterizza il rapporto contrattuale, in aggiunta all'evidente interesse patrimoniale degli operatori economici del mondo digitale. La qualificazione delle operazioni negoziali in cui si inserisce una prestazione di consenso al trattamento dei dati personali, probabilmente in termini

Ma lo scenario si presenta più complesso⁹.

Lo strumento informatico, potendo attingere a una costellazione di fonti (*database*, motori di ricerca, negozi virtuali, e-mail, *social network*, servizi *cloud/storage*, le cose stesse nell'*Internet of Things*¹⁰), è in grado di aggregare e analizzare un tale ammontare di dati, impensabile per la mente umana, e di produrne di ulteriori, in virtù dell'incrocio delle informazioni a disposizione.

Fanno così ingresso nella società dell'informazione i *big data: dataset* che per la loro estensione in volume, velocità e varietà, tramite l'uso degli algoritmi, consentono di estrarre informazioni aggiuntive, di elaborare risultati con altissimo grado di certezza, tali da determinare modelli di *business* e mercati, utilizzi scientifici di questo sapere digitale, orientare comportamenti collettivi¹¹. I dati personali, che entrano nella disponibilità di una molteplicità di soggetti pubblici e privati, sono poi elaborati da coloro che hanno i più estesi *database* (motori di ricerca), che si vengono a trovare in posizioni quasi monopolistiche o, in ogni caso, dominanti.

somministrazione di servizi, oltre a porre in risalto la requisito della onerosità/gratuità (sul tema, in generale, L. GATT, *La liberalità*, I, Torino, Giappichelli, 2002, p. 309 ss.), richiama in senso problematico ma sostanziale le più ampie questioni sulla *commodification* dei dati personali, su cui per tutti, G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, Jovene, 2005. Più di recente, G. F. AJELLO, *La protezione dei dati personali dopo il trattato di Lisbona. Natura e limiti di un diritto fondamentale «disomogeneo» alla luce della nuova proposta di General Data Protection Regulation*, in *Osservatorio di dir. civ. comm.*, il Mulino, 2015, p. 421 ss. spec. 443, alla luce della nuova disciplina europea, richiama le teorie "proprietarizzanti" sui dati personali.

9 Lucidamente individua il collegamento tra le diverse fasi dello sviluppo tecnologico e contenuti della regolamentazione in materia di protezione dei dati personali A. MANTELERO, *The Future of Consumer Data Protection*, cit.

10 Sull'IoT, preliminarmente, P. PAGANINI, *Verso l'internet delle Cose*, in *Dir. ind.*, 2015, p. 107 ss.

11 L'estrazione di valore nei *big data* avviene attraverso metodi analitici di *data mining* (algoritmi). Gli *analytics* sono strumenti di tracciamento dei dati: software che permettono di trovare correlazioni tra dati, analizzare serie storiche, determinare trend e comportamenti stagionali, simulare scenari economici, segmentare clienti e condurre attività di *data e text mining* per comprendere meglio una vasta gamma di fenomeni di business. Si tratta di strumenti che permettono ai decisori di aziende private e pubbliche di prendere decisioni migliori. Prevedere gli indicatori di budget in base alle serie storiche, capire in anticipo il comportamento di clienti e dipendenti, valutare il grado di rischio di un finanziamento, sono alcuni esempi pratici di uso degli *analytics*. In tema, si vedano: G. D'ACQUISTO e M. NALDI, *Big data e privacy by design*, Torino, Giappichelli, 2017, spec. p. 27; R. MORO VISCONTI, *Valutazione dei big data e impatto su innovazione e digital branding*, in «Rivista di diritto Industriale», 2016, p. 46 ss.

La più frequente e redditizia attività di elaborazione è rappresentata dalla profilazione delle persone fisiche, la quale, tramite la cronologia delle loro attività, siano o meno rese anonime o pseudo anonime, consente di elaborare preferenze, interazioni, stili di vita. Essa può essere utilizzata al fine di proporre prodotti o pubblicità mirata; al monitoraggio predittivo di più ampi gruppi sociali¹²; all'incrocio e alla correlazione di fenomeni del più disparato genere con alti livelli di probabilità e con impatto notevole sul rapporto tra privati e di questi con la pubblica amministrazione¹³. Queste attività, che costituiscono una fase preliminare al rapporto tra produttore e consumatore, stanno segnando un vero passaggio d'epoca in termini di sviluppo economico e di controllo sociale¹⁴.

2. Le scelte di regolazione. Ragioni e ambito della presente indagine

La formazione di nuovi mercati di “beni”, influenzata sempre più incisivamente dallo sviluppo tecnologico¹⁵, ha determinato la necessità di apposita regolazione. In ambito europeo, a partire dagli

12 Il Garante Privacy nelle *Linee guida in materia di trattamento di dati personali per profilazione on line*, 19 marzo 2015, n. 161, [doc. web n. 3881513], definisce la profilazione come «l'analisi e l'elaborazione di informazioni relative a utenti o clienti, al fine di suddividere gli interessati in “profili”, ovvero in gruppi omogenei per comportamenti o caratteristiche sempre più specifici, con l'obiettivo di pervenire all'identificazione inequivoca del singolo utente (cd. single out) ovvero del terminale e, per il suo tramite, anche del profilo, appunto, di uno o più utilizzatori di quel dispositivo»; ed essa è finalizzata: alla messa a disposizione di servizi sempre più mirati e conformati sulle specifiche esigenze dell'utente; alla fornitura di pubblicità personalizzata, all'analisi e monitoraggio dei comportamenti dei visitatori dei siti web; allo sfruttamento commerciale dei profili ottenuti, i quali possono avere un significativo valore di mercato in ragione della loro capacità di fornire indicazioni sulle propensioni al consumo di beni e servizi.

13 Com'è stato nel caso della mappatura della diffusione dell'influenza da parte di Google in tempo reale e 2 settimane prima delle istituzioni governative, ottenuta semplicemente attraverso un'analisi delle parole chiave maggiormente digitate dagli americani in un dato periodo. Sul punto, M. BOGNI – A. DEFANT, *Big data: diritti IP e problemi della privacy*, in «Rivista di diritto industriale», 2015, p. 117 ss.

14 L'incidenza dei processi comunicativi nelle relazioni economiche della società contemporanea è chiara nell'analisi che viene fatta dalla cd. economia della comunicazione. Si veda G. SANGIULIANO, voce *Economia della comunicazione*, in *Enciclopedia Treccani online*, XXI sec., disponibile su www.treccani.it

15 Cenni al tema “classico” del rapporto tra sviluppo tecnologico, economico, normativo sono in F. DI PORTO, *Dalla convergenza digitale-energia l'evoluzione della specie: il consumatore «iper-connesso»*, in «Mercato e concorrenza», 2016, p. 59 ss. spec. 61, nt. 9.

anni novanta, il problema regolatorio è stato affrontato intorno al rapporto tra principio della libera circolazione dei dati personali e diritto (fondamentale) delle persone fisiche sui propri dati inteso come libertà fondamentale¹⁶, con una dettagliata legislazione mirante alla protezione di tali dati personali.

Secondo l'impostazione che vede il diritto sui propri dati come libertà fondamentale (sebbene non prerogativa assoluta), è stato così riconosciuto alle persone, i cui dati sono oggetto di operazioni da parte di terzi, il diritto ad essere informati di tali trattamenti, a poterne spesso autorizzare o meno l'utilizzo; in ogni caso, a controllare e gestire l'utilizzo di tali informazioni.

Nello spazio giuridico europeo, è questa formalizzazione dell'interesse del singolo ai propri dati personali in termini di libertà fondamentale a giustificare che la liceità delle operazioni aventi ad oggetto dati sia consentita solo in presenza del consenso dell'interessato, oltre che di altre condizioni normativamente previste: un interesse pubblico, la necessità rispetto alla realizzazione di altri diritti fondamentali («base giuridica» – secondo il Regolamento o «condizioni di liceità»). Ma l'attività di chi effettua operazioni su, o tramite, dati personali è sottoposta, altresì, ad altri limiti per l'accesso e l'utilizzo dei dati, come i principi di finalità, necessità e proporzionalità, la tipologia di dati trattati; regole di gestione (misure di sicurezza) volte a garantire la non dispersione, l'utilizzo conforme a quanto autorizzato dall'interessato e a obblighi di legge o amministrativi; un controllo (*ex ante* ed *ex post*) da parte di autorità indipendenti; sanzioni civili, amministrative, penali.

Tale "architettura di protezione" ha tra i suoi perni fondamentali l'autodeterminazione, libera e informata, del singolo a consentire l'accesso dei propri dati da parte di terzi privati e a mantenerne il controllo e il potere di intervento (consenso quale primario fondamento legittimo di trattamento, *ex art. 8, co. 2 Carta Nizza*), come ribadito dai più

16 Gli obiettivi perseguiti anche dal Regolamento (UE) 2016/679 (come si vedrà, l'ultimo e incisivo provvedimento in sede europea), al pari della normativa pregressa, sono rappresentati dalla libera circolazione dei dati all'interno del mercato europeo e dalla tutela delle persone (come evidente dallo stesso titolo del provvedimento normativo nonché art. 1, cons. 170, cons. 6, cons. 13)

recenti provvedimenti normativi in materia¹⁷. Tuttavia, essa risponde evidentemente anche ad un'opzione di tutela della società di cui la persona fa parte, attraverso una scelta di *policy* che intende limitare la dispersione o diffusione di dati personali, come si evince dalle altre "basi giuridiche" di trattamento richieste nonché dai principi che presidiano il trattamento e dall'apparato sanzionatorio.

A cospetto del binomio tutela della persona e tutela della società, appare allora lecito interrogarsi se una scelta normativa che ponga al centro, comunque e per un elevato numero di trattamenti, l'autodeterminazione della persona in una realtà sempre più dominata dalla strumentazione tecnologica possa dirsi realistica ed efficace rispetto agli obiettivi di tutela. Se quasi ogni atto di relazione interpersonale è caratterizzato da un trattamento digitalizzato¹⁸, con le evidenti conseguenze che possono derivarne in termini di capacità di attenzione e controllo, sono la consapevolezza e l'autonomia della decisione, cioè un consenso, che si voglia pure formalmente espresso, libero, informato e specifico, gli strumenti idonei a tutelare il singolo e la società?¹⁹

Alla presumibile irrealizzabilità di atti di autodeterminazione e controllo che consentano al singolo di mettere in pratica la pur percepita importanza della propria sfera personale, si aggiungano due ulteriori profili. Come si è visto, la produzione di informazioni relative alla persona può prescindere dal singolo consenso prestato, com'è nel caso dei risultati dell'elaborazione algoritmica di altri dati personali, ove in qualcuna delle innumerevoli prestazioni di consenso richieste si sia autorizzata la profilazione (anch'essa oggetto di specifica approvazione). Qual è dunque la concreta possibilità di controllo del singolo sulla propria sfera personale? Infine, anche laddove si

17 Il potere di autodeterminarsi viene, correntemente, letto quale principio informatore dell'esercizio dei diritti della persona a più ampio spettro, come libertà di autodeterminazione nelle scelte inerenti i diritti inviolabili della persona. Nel senso di un chiaro principio comune consistente nell'autonomia delle scelte personali in ambito di libertà della persona, anche nella sua dimensione fisica (diritto alla salute, oltre che libertà di pensiero, religione, associazione etc.), G. FERRANDO, *Consenso informato del paziente e responsabilità del medico, principi, problemi e linee di tendenza*, in «Rivista critica di Diritto privato», 1998, p. 37, spec. pp. 39 e 44 s.

18 L'osservazione è di F. Pizzetti, nell'introduzione a D'Acquisto e Naldi, *op. cit.*, p. XIII.

19 Secondo la normativa vigente, nel caso in cui il trattamento sia operato da un soggetto privato, ex art. 23 cod. privacy.

continuasse a valorizzare il consenso come diritto di scelta che sia espressione di una libertà fondamentale, sempre in un'ottica di politica del diritto, quali sono le possibilità che tale strumento possa realizzare anche l'aspirazione di coloro che con atti di diniego intendano escludere il trattamento dei propri dati?

La retorica (e/o la sostanza) del diritto alla protezione dei dati personali come libertà fondamentale non può impedire di valutare l'idoneità dello strumentario giuridico utilizzato e di contestualizzarlo nello scenario tecnologico attuale.

Può valere la pena, allora, porsi in prospettiva critica rispetto alle opzioni più di recente valorizzate (come il consenso al trattamento dei dati personali) dal legislatore europeo (il Regolamento (UE) 2016/679)²⁰ per verificarne i limiti, ovvero possibili scenari alternativi (prospettiva de *iure condendo*).

Il livello di analisi, cui si farà riferimento, è duplice:

1. da un lato si verificherà se lo strumento di regolazione e tutela previsto (il consenso) sia funzionale ai dichiarati obiettivi della tutela stessa (la scelta consapevole da parte della persona fisica acchè avvenga il trattamento e il controllo sui dati trattati²¹). Questa prima fase prevede, in particolare, l'analisi di alcuni risultati che attingono alle scienze psico-comportamentali con particolare riguardo all'attitudine degli individui rispetto alla manifestazione del consenso al trattamento di dati personali²²;
2. tenuto conto del risultato del primo livello dell'analisi, si procederà ad esaminare il contenuto del diritto alla protezione dei dati, verificandone la portata (o la semantica) sotto il profilo rimediale delle tutele civili.

²⁰ Pur non essendo ancora stato emanato uno specifico provvedimento avente ad oggetto le comunicazioni elettroniche (in sostituzione della direttiva 2002/58/CE), il Regolamento (UE) 2016/679 in GUUE L119 del 4 maggio 2016, entrato in vigore il 24 maggio 2016, (la cui disciplina si applicherà a decorrere dal 25 maggio 2018 (art. 99, par. 2)), tiene conto della neutralità tecnologica (cons. 15).

²¹ Cons. 7 reg. (UE) 2016/679.

²² In generale sugli studi comportamentali nella dottrina giuridica, v. tra gli altri L. ARNAUDO, *Diritto cognitivo. Prolegomeni a una ricerca*, in «Politica del diritto», 2010, p. 101 ss.; B. LURGER, *Empiricism and Private Law: Behavioral Research as Part of a Legal-Empirical Governance Analysis and a Form of New Legal Realism*, in «Australian Law Journal», 2014, p. 19 ss.

Ciò potrebbe portare a configurare non solo una diversa graduazione della tutela dei dati rispetto alla loro incidenza sui diritti fondamentali dell'individuo, ma a ipotizzare meccanismi di tutela diversi da quelli attuali²³.

3. Circolazione e protezione dei dati personali nella realtà tecnologica: le scelte del legislatore europeo e il Regolamento (UE) 2016/679

Nel quadro della complessiva regolamentazione del trattamento dei dati personali, l'adozione del Regolamento (UE) 2016/679 (*General Data Protection Regulation* o GDPR)²⁴ ha impresso una nuova marcia alla già articolata disciplina prevista a livello europeo e nazionale²⁵, al fine di rispondere agli sviluppi tecnologici e ai nuovi modelli di crescita economica (cons. 6) con regole di protezione tecnologicamente neutrali, che si applicano cioè a prescindere dalla tecnica utilizzata e dall'automatizzazione o meno del trattamento (cons. 15).

Mentre viene conservato, pur con alcune modifiche, l'apparato definitorio e dei concetti fondamentali relativamente all'individuazione e ruoli dei soggetti coinvolti, e dei loro diritti e doveri, il Regolamento 2016/679 modifica l'impianto di fondo delle regole del trattamento dei dati personali, proprio della direttiva 95/46/CE (cd. direttiva madre) e della legislazione interna, con riguardo ai modelli organizzativi e

23 In sintesi, v'è da chiedersi: quali siano, al di fuori della formula del diritto alla protezione dei dati personali, gli interessi tutelati come libertà fondamentale e come interesse della collettività; se gli strumenti predisposti dall'ordinamento siano efficaci rispetto alla protezione di tali interessi; quali le possibili proposte alternative *de iure condendo* ovvero in sede di interpretazione.

24 Tra i primi commenti L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il Regolamento Privacy europeo*, Milano, Giuffrè, 2016; *Privavy Protezione e trattamento dei dati*, a cura di M. Soffientini, Milanofiori Assago, Wolters Kluwer, 2016; *Il regolamento generale sulla tutela dei dati personali*, a cura di S. Sica, V. D'Antonio, G. M. Riccio, Padova, Wolters Kluwer, 2016; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, II, Torino, Giappichelli, 2016.

25 Per l'ordinamento europeo, la cd. direttiva madre Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati Direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno, entrambe recepite nell'ordinamento interno, ora nel d. lgs. 30 giugno 2003, n. 196 (cd. cod. *privacy*).

imprenditoriali e agli adempimenti in capo ai titolari e responsabili²⁶.

Ridotti gli adempimenti di carattere amministrativo (nonostante riemersione di obblighi di compilazione di documenti che registrino le attività trattamento)²⁷, i trattamenti, alle condizioni di legge, sono condotti “a rischio” del titolare e degli altri soggetti di volta in volta previsti²⁸. Il Regolamento non manca di individuare una serie di misure da adottare, in capo al titolare aventi carattere tendenzialmente preventivo, ma si tratta di prescrizioni che ribaltano sull'organizzazione aziendale e su strumenti a loro volta tecnologici la finalità di protezione. Si pensi alla valutazione d'impatto o *Privacy Impact Assessment* (cons. 84 ss. e art. 35 ss.), in caso di rischio elevato per diritti, libertà, persone fisiche; la progettazione di sistemi e applicative finalizzati alla minimizzazione dell'uso di dati personali (ccdd. *Privacy by design e by default* - art. 25), misure tecniche e organizzative volte a minimizzare il rischio per i dati personali (come pseudonimizzazione)²⁹; la nomina obbligatoria, in taluni casi³⁰, di una nuova figura di controllo, *Data Protection Officer* o responsabile della protezione dei dati personali (art. 37 ss., cons. 97): un manager, del quale si richiede una posizione terzietà e una funzione di consulenza a responsabile/titolare, al fine di assicurare una gestione corretta in imprese ed enti e fungere da punto di contatto autorità.

Si tratta di misure che hanno il compito di responsabilizzare (*accountability*) il comportamento del titolare (art. 24 e art. 2) verso l'adozione di procedure in grado di evitare rischi per i dati, a pena di elevate sanzioni amministrative pecuniarie (art. 83 ss.) (fino al 4% fatturato mondiale annuo dell'esercizio precedente); o – ma qui,

26 G. GIANNONE CODIGLIONE, *Risk-based approach e trattamento dei dati personali*, in *Il regolamento generale sulla tutela dei dati personali*, cit., p. 56 ss.; A. CICCIA MESSINA e N. BERNARDI, *Privacy e regolamento europeo*, Milanofiori Assago, Ipsoa, 2016. Si stima che il 60/70% delle norme del codice privacy verranno disapplicate con l'applicazione del Regolamento nel 2018.

27 L'art. 30 prescrive un obbligo di compilazione del registro per il titolare e il responsabile, il quale, sebbene non si applichi a tutti i titolari, fa rivivere gli obblighi già in passato prescritti dall'ordinamento italiano e relativi al documento programmatico di sicurezza, poi abolito dal D.l. n. 5 del 9 febbraio 2012, convertito dalla legge n. 35 del 4 aprile 2012.

28 Alla riduzione degli oneri amministrativi per i responsabili del trattamento fa riferimento il considerando 89.

29 Ma già in art. 17 cod. privacy.

30 La figura del DPO è obbligatoria per i soggetti pubblici o in caso di trattamenti che richiedono monitoraggio regolare e sistematico su larga scala ovvero in caso di dati sensibili o giudiziari.

però, senza innovazioni di rilievo – risarcimenti (art. 82). Nel senso di accresciuta deterrenza, può essere interpretato l'inasprimento delle sanzioni amministrative; e nel senso di un miglioramento dei modelli organizzativi sono le norme che promuovono certificazioni e organismi di certificazione (art. 42 s.), codici di condotta e meccanismi di certificazione rilasciati da un soggetto abilitato o dall'autorità di protezione dati (art. 35 ss.).

A tali misure si accompagnano: l'affermazione di diritti in capo alle persone fisiche (oblio, portabilità – art. 20); la regolazione uniforme all'interno del mercato unico del trattamento dei dati di chi si trovi sul territorio dell'Unione Europea³¹, garantita da un'autorità europea, lo *European Data Protection Board* (Comitato) (art. 68), che sia affianca al già esistente *European Data Protection Supervisor* e alle autorità garanti nazionali; e, fuori dallo spazio europeo, la limitazione della circolazione dei dati in base alla valutazione di conformità delle misure garantite, per i dati trasferiti extra-UE³².

Le scelte normative sopra indicate rivelano un'impostazione volta a non impedire le prospettive tecnologiche di produzione sempre più massiva di dati, le sfere di utilizzo e le tecniche che consentono la moltiplicazione dei dati stessi, ma a disciplinare i trattamenti con meccanismi, ritenuti "virtuosi", finalizzati a minimizzare i rischi di perdita, dispersione, diffusione, nella dichiarata finalità di proteggere la sfera dei soggetti cui i dati si riferiscono.

La tecnologia (*privacy by design*, tramite *anonimizzazione* e *pseudoanonimizzazione*) viene chiamata a disciplinare la tecnologia (essendo i trattamenti, ormai, quasi del tutto automatizzati) secondo gli obiettivi predisposti dal legislatore, mentre le regole giuridiche guadagnano un proprio spazio importante in punto di disciplina sanzionatoria.

31 Quanto all'ambito di applicazione territoriale della normativa (artt. 3 – 5): non si fa più riferimento alla collocazione del terminale nello Stato Membro, ma all'offerta dei servizi in stati UE, per cui la nuova disciplina si applica integralmente alle imprese situate fuori dall'Unione europea che offrono servizi o prodotti a persone che si trovano nel territorio dell'Unione europea.

32 E' prescritta l'osservanza di procedure e adeguatezza per il trasferimento dei dati extra-Ue, o, in mancanza, il consenso esplicito dell'interessato o altre particolari condizioni.

Resta, tuttavia, da verificare se, da un lato, le regole tecniche che spettano ai titolari scegliere e predisporre si dimostrino efficienti, mentre, quanto agli strumenti giuridici di protezione, se un accorto utilizzo del potere sanzionatorio da parte delle Autorità garanti sia in grado di assolvere la funzione deterrente voluta.

Il Regolamento – come detto – non incide sull’assetto del mercato – oligopolistico – oggi esistente in materia di dati personali, che peraltro per le sue caratteristiche ostacola l’ingresso di nuovi attori, né su alcune fondamentali incoerenze di approccio, com’è nel caso della profilazione³³ quale emblematica espressione di trattamento automatizzato, oggetto anch’esso di puntuale informazione, autorizzazione e diritto di opposizione.

4. Il “consenso” come base giuridica per il trattamento dei dati personali secondo il Reg. (UE) 2016/679

Come anticipato, con riguardo alla funzione assegnata al “consenso informato”, la nuova normativa europea, pur introducendo alcune modifiche, non innova significativamente il quadro preesistente, risultante dalla prima direttiva in materia (la cd. direttiva madre 95/46/CE) e della sua attuazione negli Stati Membri, in particolare in Italia³⁴.

Il consenso è solo uno dei “fondamenti legittimi” (secondo la terminologia della Carta di Nizza, o base giuridica) per il trattamento

33 Art. 4, n. 4, conss. 60, 63, 70, 71, 72, artt. 13, para. 2, lett. f) art. 14, para. 2, lett. g) del Regolamento e art. 14 cod. privacy

34 Senza volerci addentrare nel novero di differenze – pur esistenti – tra i diversi testi normativi, può osservarsi come, in punto di *design*, il Regolamento riprenda la struttura della direttiva cd. madre includendo il consenso tra le condizioni di liceità dei trattamenti in generale (art. 6 GDPR, e art. 7 direttiva madre che parlava di principi relativi alla legittimazione del trattamento) o tra le deroghe al divieto di trattamento per «particolari categorie di dati» (leggi *dati sensibili*, art. 9 GDPR e art. 8 direttiva madre). Diversamente, il legislatore italiano, avendo distinto la disciplina dei trattamenti in base ai soggetti, ha reso il consenso regola solo per i trattamenti effettuati da soggetti privati ed enti pubblici economici (art. 23), con particolari garanzie in caso di dati sensibili. Questi ultimi, quando trattati da soggetti pubblici, sono sottoposti a particolari principi e autorizzazioni ma, dalla normativa primaria, non al consenso.

dei dati personali³⁵, sia con riguardo ai dati personali in generale (ove il consenso è condizione di liceità, ex art. 7) sia con riguardo a particolari categorie di dati (ove esso esclude il divieto di trattamento, art. 9)³⁶.

Ora definito come «espressione di 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, acchè i dati personali che lo riguardano siano oggetto di trattamento» (art. 4, par. 1, n. 11, Reg. 2016/679)³⁷, il consenso è nel nuovo testo normativo più chiaramente valorizzato in senso attivo/positivo (ma non necessariamente scritto), sebbene non manchino – nel quadro di previsioni normative tecnologicamente neutrali – alcuni contemperamenti per il caso di utilizzo di mezzi elettronici, ove è comunque richiesta un'azione positiva di accettazione³⁸. In proposito, si deve aver in mente non solo

35 Si conferma, quindi, come un ampio settore del trattamento dei dati resti sottratto alle regole del consenso. Il consenso continua a rappresentare una soltanto delle basi legittimanti il trattamento, richiesto ove non sia necessario per l'esecuzione di un contratto o la fase precontrattuale, per l'adempimento di un obbligo di legge per il titolare, per la salvaguardia di interessi vitali, per l'adempimento di compiti di interesse pubblico o l'esercizio di pubblici poteri, per il perseguimento di un *interesse legittimo* del titolare o di un terzo purchè non confliggenti con i diritti dell'interessato (art. 7 GDPR). Significativa apertura per il mercato, in proposito, è la possibilità che il trattamento di dati personali per finalità di marketing diretto sia considerato perseguimento di un legittimo interesse del titolare del trattamento o terzi (cons. 47). Quanto alle particolari categorie di dati, sono previste anche in questo caso specifiche deroghe ulteriori rispetto al consenso (art. 9 GDPR). Sulla diversa struttura delle condizioni di liceità nel codice privacy e nel Regolamento (e nella dir. 95/46/CE), L. BOLOGNINI, E. PELINO, *Condizioni di liceità*, in L. BOLOGNINI, E. PELINO, C. BISTOLFI, *op. cit.*, p. 278 s., ma essa non determina apprezzabili conseguenze sul piano applicativo.

36 Nel mantenimento del meccanismo informativa + consenso, si conferma la necessità di un consenso inequivocabile (esplicito per dati sensibili) e su richiesta (come in materia di consumatore sono escluse le caselle *pre-ticked*), favorito anche dalla presenza di icone (identiche in UE), anche relativamente al trasferimento dei dati extra-UE e all'esistenza del diritto di revoca (cons. 32 ss., artt. 6-8). Sul diritto alla *privacy* quale autodeterminazione (come controllo sulla raccolta, sulla diffusione, sull'elaborazione sulla correttezza e sulla rimozione del dato) già nel sistema ante-regolamento, G. SARTOR, *Privacy, reputazione, affidamento: dialettica e implicazioni per il trattamento dei dati personali*, in *Privacy digitale. Giuristi e informatici a confronto*, Torino, Giappichelli, 2005, 81 ss.

37 Recita il vigente art. 23 cod. privacy: «Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'art. 13».

38 Considerando 32, segnatamente nella parte in cui fa rinvio a «qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non

l'utilizzo di strumenti digitali ma, inevitabilmente, la già dilagante diffusione dei sensori (es. software di rilevamento del movimento, rilevamento touch, etc.).

Permane la qualificazione di «consenso esplicito» solo con riguardo ai dati sensibili, ove per questi il consenso sia richiesto (art. 9 GDPR e art. 8, par. 2, lett. *a*) direttiva madre). Una manifestazione esplicita di consenso è prevista anche ai fini di profilazione (art. 22 GDPR) e in caso di trasferimento presso un paese terzo o un'organizzazione internazionale (art. 49, par. 1, lett. *a*). Consenso esplicito può intendersi come consenso non solo non desumibile da comportamenti concludenti (espreso), ma che sia chiaramente manifestato. Si tratta di una qualificazione ulteriore e diversa dal consenso espresso (cioè non tacitamente manifestato, coerentemente ad un'interpretazione sistematica secondo il diritto italiano³⁹), tale dovendo essere qualsiasi consenso, sia per il legislatore europeo (cons. 32), sia per il legislatore italiano (art. 23 cod. privacy)⁴⁰. Non è più prescritto specificamente, tuttavia, alcun requisito di forma *ad substantiam* nè autorizzazione del Garante, come, invece, era stato introdotto con riguardo ai dati sensibili dal legislatore nazionale (art. 26 cod. priv.).

Permane l'obbligatorietà di una trasparente informativa. Il consenso, secondo uno schema che richiama quello del neoformalismo negoziale (o comunque dell'agire giuridico) in diversi settori, deve far seguito ad un novero di informazioni obbligatorie fornite all'interessato⁴¹. L'informazione resta comunque dovuta, anche quando

dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle [...]. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso».

39 F. GALGANO, *Il contratto*, II ed., Padova, Cedam, 2011, p. 126.

40 L'espressione *consenso espresso* si riferisce in entrambi i testi normativi al consenso comunque richiesto. In proposito E. PELINO, *I diritti dell'interessato*, in L. BOLOGNINI, E. PELINO, C. BISTOLFI, *op. cit.*, p. 223, il quale tuttavia opera una diversa interpretazione. A nostro modo di vedere il precetto di un consenso esplicito introduce solo una maggiore determinatezza nel contegno. Si veda in proposito anche S. THOBANI, *I requisiti del consenso al trattamento dei dati personali*, Santarcangelo di Romagna, Maggioli, 2016, p. 33 s.

41 Alcune riflessioni sul ruolo dell'informazione in funzione della manifestazione del consenso al trattamento dei dati personali sono riferite più avanti, al par. 5.

non sia propedeutica ad una successiva manifestazione di volontà⁴².

Tra i tratti più innovativi del Regolamento in tema, vi è la previsione relativa alla capacità del minore sedicenne e ultra-sedicenne (o di età inferiore, secondo le legislazioni nazionali) di prestare il consenso al trattamento dei dati, ove richiesto nell'ambito dei servizi della società dell'informazione (art. 8 GDPR)⁴³. Per il minore di età inferiore si prevede singolarmente, in via alternativa, la rappresentanza dell'esercente la responsabilità genitoriale o la sua autorizzazione rispetto alla manifestazione di volontà del minore. La disposizione lascia insoddisfatti per due ragioni: non intercetta la realtà attuale in cui i minori infrasedicenni operano in rete quasi esclusivamente in via autonoma, riuscendo spesso ad aggirare ogni tipo di restrizione all'accesso, come, ad esempio, dichiarando una diversa data di nascita⁴⁴. La richiesta di una prestazione del consenso da parte del genitore (che dovrebbe, presumibilmente, autenticarsi con proprio ID e password) al momento dell'accesso, e per prestazioni diverse da quelle necessarie all'esecuzione del contratto (nel qual caso rileverà la valutazione della capacità necessaria per concludere il contratto), non comporta di per sé l'obbligo di determinare restrizioni nella navigazione e quindi non è detto sia in grado di tutelare i minori, non solo dai pericoli della rete. Va poi considerato sempre l'effetto "di rete", per cui può avvenire che l'autorizzazione la trattamento data dal genitore in un caso (es. per l'iscrizione ad un *social network*) sia poi posta nel nulla per effetto di successive autorizzazioni al trattamento dei propri dati personali date dal

42 La trasparenza, oltre ad essere principio generale del trattamento (art. 5, par. 1, lett. a) è qualificazione dell'informazione che il titolare deve fornire all'interessato in ogni caso, anche ove il consenso non sia richiesto. Particolare attenzione in termini di chiarezza e comprensibilità è richiesta nei riguardi degli interessati minori (art. 12 GDPR). Sull'informativa, sebbene non espressamente prescritta come trasparente, già art. 13 cod. privacy.

43 Con specifico riguardo al consenso del minore G. SPOTO, *Disciplina del consenso e tutela del minore*, in *La nuova disciplina europea della privacy*, a cura di S. Sica, V. D'Antonio, G. M. Riccio, Padova, 2016, p. 111 ss., nonché S. THOBANI, *op. cit.*, p. 13 ss.

44 L'affermazione contenuta nel testo prescinde dalle valutazioni circa l'applicabilità dell'art. 1426 c.c. all'ipotesi della dichiarazione del minore di essere maggiorenne (secondo un'interpretazione estensiva della norma che comprenda ipotesi diverse dal raggirio in senso stretto). Riguarda, invece, l'opportunità di una previsione relativa all'età dell'interessato quale strumento di tutela a protezione dello stesso. Sull'applicazione diretta o analogica della disposizione citata e in generale della disciplina del contratto al consenso al trattamento, si veda *infra* par. successivo.

minore quando utilizza applicazioni che richiedono l'accesso o utilizzano le informazioni dei profili *social*⁴⁵. Appare chiaro che, anche in questo caso, la previsione normativa va integrata con il *design* tecnologico, anche in una prospettiva di interrelazione tra le applicazioni.

Inoltre, la previsione, limitata ai servizi elettronici, non chiarisce in via generale i requisiti di capacità del minore con riguardo alla prestazione del consenso al trattamento dei propri dati.

La previsione di speciali condizioni di liceità per la prestazione del consenso dei minori nel campo dei servizi elettronici sembra rispondere, nell'intenzione del legislatore, all'esigenza di fornire un criterio generale rispetto a trattamenti che, per numero e tipologie, non consentono un accertamento delle capacità di discernimento dell'interessato in relazione al contenuto del consenso.

Infatti, su un piano più generale, il problema della capacità richiesta per la prestazione del consenso non trova univoca soluzione in considerazione della qualificazione sia non patrimoniale (in quanto incidente su interessi della persona) sia patrimoniale (per il valore di scambio dei dati personali) degli interessi coinvolti. Il discorso si sposta, allora, sul più ampio problema del consenso del minore nell'ipotesi in cui l'esercizio di una libertà comporti un atto dispositivo, anche in considerazione del valore economico dello stesso, ponendosi la questione se dunque sia sufficiente la mera capacità d'intendere o volere, anche per gli atti di natura patrimoniale correlati alla manifestazione di una libertà della persona, ovvero anche la capacità di agire⁴⁶.

45 L'identificazione del minore pone di fronte all'ambiguità propria della protezione dei dati personali nella società dell'informazione. In una dimensione potenzialmente anonima, o tale da consentire il mascheramento (come Internet), la tutela di particolari soggetti deboli, per essere effettiva, dovrebbe passare attraverso un sistema di identificazione (anche biometrica), ma ciò, a ben vedere, comporterebbe una condivisione indefinita di dati personali.

46 Nel senso della sufficienza della sola capacità d'intendere e di volere, S. PATTI, *Consenso*, sub art. 23), in *La protezione dei dati personali. Commentario*, a cura di C.M. Bianca e F. D. Busnelli, t. I, Padova, Cedam, 2007, p. 541 ss., spec. pp. 544-546. La tematica è complessa e pone il problema dell'applicabilità analogica delle discipline speciali in materia di lavoro o di tutela del diritto di autore. Sul punto, più estesamente, S. THOBANI, *op. cit.*, p. 13 ss., anche per la bibliografia rilevante e *infra* al paragrafo successivo.

5. Natura giuridica e ruolo del consenso nella complessiva operazione negoziale

L'accertamento della capacità con riguardo all'atto espressione del consenso al trattamento induce ad una più ampia indagine sulla qualificazione giuridica di quest'ultimo.

Il dibattito relativo alla negoziabilità o meno dell'atto del consenso, che pure ha sollevato sin dalla prima legge sulla protezione dei dati raffinate riflessioni⁴⁷, ha un rilievo applicativo sostanzialmente marginale, non solo in virtù della crisi di tale categoria dogmatica, ma, in particolare, per l'esistenza della disciplina speciale sul consenso qualificato (come espresso, informato, libero, inequivocabile, specifico) al trattamento⁴⁸. Potenziali ricadute dell'adesione all'una piuttosto che all'altra tesi possono riguardare, appunto, la verifica dei requisiti di capacità necessari (pur non essendo decisive le soluzioni, data la complessità dei criteri riguardanti l'agire giuridico del minore); l'applicazione analogica o diretta, se compatibile, della disciplina del contratto ovvero dell'applicazione analogica di altri statuti disciplinari, come la normativa sul diritto d'autore.

Tuttavia, alcuni aspetti che emergono da tale dibattito possono aiutare a meglio comprendere l'effettivo ruolo del consenso nella strategia di protezione dei dati personali.

Il dato personale tende a rivestire una duplice valenza. In base al potenziale impatto del suo utilizzo sulle libertà fondamentali e alla protezione che riceve nello spazio giuridico europeo tramite la libertà alla protezione dei dati⁴⁹, esso costituisce riferimento oggettivo di situazioni giuridiche di natura non patrimoniale. Allo stesso tempo, può essere oggetto di diritti patrimoniali, in ragione della sfruttabilità economica dei diritti sui dati, essendo consentiti di questi ultimi l'utilizzo e la circolazione anche a titolo oneroso (si pensi utilità economiche

47 V. CUFFARO, *Il consenso dell'interessato*, in *La disciplina del trattamento dei dati personali*, V. Cuffaro, V. Ricciuto, Torino, Giappichelli, 1997, p. 204 ss.

48 Sulla irrilevanza degli altri profili S. PATTI, *op. cit.*

49 Ulteriori considerazioni critiche sulla concettualizzazione di un autonomo diritto alla protezione dei dati sono espresse *infra* al par. 7.

ricavabili dai dati da parte dell'interessato e, in maniera più rilevante, dal titolare)⁵⁰. Si tratta di ambivalenza che è ben nota con riguardo a vari diritti della personalità⁵¹.

Questa duplicità di rilevanza giuridica s'interseca, come anticipato, con la qualificazione del consenso come integrante un atto non negoziale nell'ambito di una più ampia disciplina a tutela del diritto sui dati, ovvero negoziale, quale negozio unilaterale a contenuto patrimoniale (ovvero non patrimoniale). Tali profili sono presenti, in vario modo, nelle tesi avanzate dalla dottrina italiana.

Partendo dalla disamina di quest'ultimo aspetto (la struttura dell'atto di prestazione del consenso), è stata proposta, in termini non negozialità, la qualificazione del consenso al trattamento dei dati personali come ipotesi di consenso dell'avente diritto (atto non negoziale, secondo l'interpretazione dominante)⁵², con funzione di scriminante l'antigiuridicità della fattispecie del trattamento dei dati⁵³. La rigorosa adesione a questo inquadramento determina che, in termini di capacità, sia sufficiente la capacità d'intendere e volere⁵⁴.

Altra dottrina, tuttavia, ha da tempo teso a riconoscere al consenso al trattamento, in via generale, il carattere di "permesso autorizzativo", con efficacia costitutiva nell'altrui sfera (personale)⁵⁵, o, secondo altra lettura, genericamente, di atto negoziale, ma sempre a contenuto non patrimoniale⁵⁶. A ben vedere, anche nel primo caso, se si vuole dare rilievo alla categoria giuridica dell'autorizzazione⁵⁷, il consenso integra

50 Sui diritti di utilizzazione economica sui diritti fondamentali (con specifico riguardo all'immagine), si tratti di aspetti dello stesso diritto o di due distinte situazioni giuridiche, C.M. BIANCA, *Diritto civile*, I, cit., p. 150 nt. 23.

51 G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 256 ss., nonché p. 279 ss.

52 C. PEDRAZZI, voce *Consenso dell'avente diritto*, in «Enciclopedia del diritto», IX, Milano, 1961, p. 140 ss., spec. p. 146 s.

53 S. PATTI, *Consenso*, sub *art. 23*), cit., p. 553 ss.

54 C. PEDRAZZI, *op. loc. cit.*

55 D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in «Rivista critica di diritto privato», 1998, p. 350 ss., spec. p. 353 s.; A. FICI – E. PELLECCIA, *Il consenso al trattamento*, in *Diritto alla riservatezza e circolazione dei dati personali*, a cura di R. Pardolesi, Milano, 2003, I, p. 485 ss., spec. p. 502.

56 F. BOCCHINI e E. QUADRI, *Diritto privato*, 6^a ed., Torino, 2016, p. 1290.

57 Sull'autorizzazione, A. AURICCHIO, voce *Autorizzazione (dir. priv.)*, in «Enciclopedia del diritto», IV, Milano, 1959, p. 502 ss., nonché L. CARIOTA FERRARA, *Il negozio giuridico nel diritto privato italiano*, Napoli, 1948 (rist. 2011), p. 711 ss., il quale tuttavia accoglie una nozione

un atto negoziale, con le relative conseguenze in termini di adattamento dei requisiti di capacità.

Per la soluzione di tale questione interpretativa, riteniamo che la lettera del dato normativo possa soccorrere, pur non essendo, da sola, decisiva.

Se si guarda all'art. 9 del Regolamento, che, come detto, riprende la formulazione della direttiva madre tuttavia non seguita nella disciplina di attuazione italiana, con riguardo alle «particolari categorie di dati» (leggi *sensibili*) sussiste un espresso divieto di trattamento, di cui il consenso esplicito e specifico da parte dell'interessato rappresenta una deroga espressa. Con riguardo, invece, al consenso relativo ai dati personali non rientranti in categorie speciali, esso è normativamente previsto quale condizione di liceità del trattamento, come di recente confermato dall'art. 7 Reg. (e di legittimazione *ex art. 7* direttiva madre)⁵⁸.

In base al dato letterale, può quindi trovare spazio, certamente con riguardo ai dati sensibili, la qualificazione del consenso al trattamento quale causa di esclusione dell'antigiuridicità, e quindi atto volontario in sé ma non finalizzato all'interesse tutelato dall'ordinamento (l'esimere da illiceità); mentre con riguardo ai dati personali il consenso fungerebbe da non meglio specificata *condicio iuris*. In proposito, si può sostenere che pur nella parziale differenza di requisiti (del consenso al trattamento dei dati personali o sensibili) e di caratteristiche dell'attività (illiceità e la liceità del trattamento come condizione di partenza), un argomento di coerenza sistematica impone di valutare in senso uniforme la prestazione del consenso, con riguardo a dati sensibili e personali, come atto giuridico in senso stretto, sempre che si voglia valorizzare tale categoria. Tale impostazione, in mancanza di dati normativi contrari, e tra l'altro secondo una ricostruzione sistematica unitaria rispetto alla

ristretta di autorizzazione come negozio attributivo del potere di disporre efficacemente in nome proprio dei diritti dell'autorizzante e sostanzialmente fonte della rappresentanza indiretta. Sull'inquadramento e fattispecie tipiche di negozio autorizzatorio M. TAMPONI, *L'atto non autorizzato nell'amministrazione dei patrimoni altrui*, Milano, Giuffrè, 1992, p. 28 ss.

58 In senso parzialmente difforme l'impostazione della normativa italiana attualmente applicabile. Il d. lgs. 196/2003 individua il consenso tra le regole per l'ammissibilità del trattamento con riguardo ai dati personali genericamente intesi (art. 23) e, con l'ulteriore requisito della forma scritta, come garanzia ulteriore in materia di dati sensibili (art. 26).

qualificazione del consenso in diversi ambiti (es. autodeterminazione terapeutica)⁵⁹, può essere accolta dall'interprete. L'atto che manifesta il consenso è quindi atto non negoziale, scriminante l'antigiuridicità o illiceità del trattamento da parte di un soggetto diverso dall'interessato nonché esercizio dell'autodeterminazione da parte di quest'ultimo. In entrambi i casi esso è condizione di legittimità del più ampio procedimento, che coinvolge una pluralità di soggetti, riguardante il trattamento dei dati.

Ciò che, però, al di fuori della qualificazione secondo categorie dommatiche, ci appare più utile segnalare è il risultato di tale interpretazione, secondo cui, in assenza di un requisito di capacità di agire richiesto in via generale, come confermato dal fatto che esso sia specificamente previsto solo con riguardo ai trattamenti automatizzati (art. 8 GDPR), l'accertamento della capacità vada correlato a quello circostanziale della autodeterminazione e non dipenda da criteri presuntivi e uniformi (capacità di agire). E tale lettura converge con il riconoscimento dell'autonomia decisionale del minore nell'esercizio dei diritti fondamentali, i cui atti di autodeterminazione prescindono da requisiti di capacità di agire.

Provando ora a fornire di contenuto sostanziale (cioè relativo agli interessi protetti) le qualificazioni formali appena indicate, queste ultime appaiono idonee a rappresentare il carattere non patrimoniale del diritto sui dati personali, come confermato dalla sua indisponibilità, e quindi inapplicabilità allo stesso dello schema obbligatorio, e dal diritto di opposizione⁶⁰ (che ha peraltro ricevuto un decisivo ampliamento dal nuovo Regolamento UE)⁶¹.

59 Per le simili questioni in tema di consenso al trattamento ed esercizio del diritto all'autodeterminazione terapeutica, v. B. SALVATORE, *Informazione e consenso nella relazione terapeutica*, Napoli, Edizioni scientifiche italiane, 2012, p. 128 ss.

60 A. DI MAJO, *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in *Trattamento dei dati e tutela della persona*, a cura di V. Cuffaro, V. Ricciuto e V. Zeno-Zencovich, Milano, Giuffrè, 1998, p. 230 ss.

61 Il diritto di opposizione passa ad essere esercitabile non più solo in caso di «motivi legittimi» (art. 7 co. 4 cod. privacy) ma di «motivi connessi alla ... situazione particolare» (art. 21, par. 1, GDPR). Nel caso di trattamenti per fini scientifici, storici, statistici tali motivi soccombono rispetto all'interesse pubblico (art. 21, par. 6). È *ad nutum* il diritto di opposizione rispetto ai trattamenti che abbiano come finalità il marketing diretto o la profilazione (art. 21, par. 2, GDPR). *La revocabilità ad nutum* è già prevista dal codice privacy in materia di servizi di comunicazione elettronica (art. 123, co. 3).

Esse, tuttavia, non valorizzano la funzione di utilità patrimoniale dei diritti sui dati personali, utilità che è stata nel tempo considerata ascritta alla sfera dei motivi, o comunque priva di rilevanza⁶², o in ogni caso non incidente sulla natura dell'atto⁶³. Così posta la questione appare argomentabile, allora, che la qualificazione del consenso, come sopra illustrata, riguardi il consenso come presupposto del trattamento, per cui non solo è elemento di una fattispecie legislativamente prevista, ma l'eventuale controprestazione corrisposta risulta irrilevante ai fini della rispondenza a tale fattispecie presa in considerazione, a meno di non incidere sul requisito della libertà⁶⁴.

Tuttavia, non può omettersi di considerare l'interesse rispetto ai dati personali nell'ambito della complessiva operazione economica in cui può inserirsi il trattamento dei dati. Il trattamento dei dati personali può entrare a far parte della causa (onerosa, gratuita) di una operazione negoziale tra titolare e interessato, diventando oggetto di una prestazione obbligatoria la cui fonte sarà un contratto (o un atto unilaterale) e la volontà che il trattamento sia eseguito confluirà nei requisiti del contratto.

Gli interessi "patrimoniali" sui dati personali possono – a nostro modo di vedere – essere valutati in un'ottica complessiva unitamente all'interesse non patrimoniale sugli stessi.

Del carattere dispositivo dell'atto che esprime il consenso al trattamento dei dati personali hanno fatto ampiamente riferimento quelle letture interpretative che, indipendentemente dal carattere oneroso o gratuito dell'operazione⁶⁵, valorizzano i dati come entità suscettibili di circolazione e di "pertinenza" alla sfera dell'interessato⁶⁶, ovvero l'efficacia derivativo-constitutiva dell'atto che stabilisce lo sfruttamento economico di attributi individuali, alla stregua di un contratto di licenza

62 S. PATTI, *op. cit.*, p. 554.

63 S. MAZZAMUTO, *Il principio del consenso e il potere della revoca*, in *Libera circolazione e protezione dei dati personali*, a cura di R. Panetta, t. I, Milano, Giuffrè, 2006, p. 993 ss., spec. 1026.

64 Il condizionamento della libertà non dipende meramente dall'esistenza di una controprestazione ma, secondo la tesi più condivisibile, dalla natura essenziale dei beni o servizi che si fanno dipendere dalla prestazione del consenso.

65 V. ZENO-ZENCOVICH, *Una lettura comparatistica della l. 675/96 sul trattamento dei dati personali*, in V. Cuffaro, V. Ricciuto e V. Zeno-Zencovich (curr.), *op. cit.*, p. 168 ss.

66 G. OPPO, *Sul consenso dell'interessato*, in V. Cuffaro, V. Ricciuto e V. Zeno-Zencovich (curr.), *op. cit.*, p. 124 ss.

nell'ambito del diritto d'autore⁶⁷.

A nostro modo di vedere, queste qualificazioni, che si focalizzano sulla patrimonialità dei dati, non escludono quelle precedentemente indicate, nell'interpretazione della legislazione speciale e a protezione del diritto sui dati personali. Vi è, infatti, un'autonomia di livelli di analisi e di piani disciplinari tra il consenso quale condizione per la liceità/legittimità del trattamento e il consenso a cedere l'utilizzo dei propri dati nell'ambito di un'operazione economica, potendo il trattamento dei dati valere o meno come prestazione in un atto economico-negoziale (come nel caso di consenso al trattamento da parte della P.A.). Quest'autonomia, che – a nostro modo di vedere – può comportare la coesistenza dei profili e delle discipline risulta confermata almeno da due dati normativi.

Uno di questi è rappresentato dalla ulteriore condizione di liceità in materia di consenso dei minori: la richiesta età superiore a 16 anni nell'ambito dei servizi della società dell'informazione ai fini di un consenso al trattamento validamente espresso non pregiudica le previsioni di legge nazionali in materia di diritto dei contratti (art. 7, ult par., GDPR). È evidente che la liceità del trattamento non comporta di per sé la validità del contratto nel quale il trattamento è eventualmente previsto.

La duplice valenza e una duplice finalità (non patrimoniale/nell'ambito delle condizioni del trattamento, patrimoniale/negoziale⁶⁸) è sottesa, poi, alla stessa previsione secondo cui può non essere richiesto un autonomo consenso al trattamento, nell'ipotesi in cui quest'ultimo sia stato già disposto in un precedente atto negoziale (contratto) o prenegoziale da parte dell'interessato (quando cioè il trattamento sia necessario per l'esecuzione di un contratto tra il titolare o l'interessato o costituisca oggetto di una richiesta precontrattuale dell'interessato (art. 24, co. 1, lett *b*) cod. privacy, art. 6, par. 1 lett. *b*) GDPR). In tal caso, il consenso contrattuale o la collocazione della richiesta nella fase pre-contrattuale assorbono la necessità del consenso al trattamento (ovvero, lo rendono nell'economia dell'operazione superfluo), pur non escludendo l'applicazione delle altre regole del trattamento, tra cui

⁶⁷ G. RESTA, *op. cit.*, p. 336.

⁶⁸ Di tale duplice profilo del consenso, già D. MESSINETTI, *op. cit.*, p. 11 ss.

l'informativa. Ma tale previsione non trova applicazione, e la diversità strutturale di atti riemerge, nel caso in cui il trattamento che sia previsto in una operazione economica riguardi i dati sensibili, ovvero quando la tipologia di trattamento non sia strettamente funzionale all'adempimento delle prestazioni dedotte in contratto. In tal caso, il consenso alle attività sui propri dati è comunque richiesto come esplicito. Qui la *ratio legis* appare essere quella di richiamare l'attenzione dell'interessato sulla scelta positiva/negativa del trattamento. In tali casi, la manifestazione di volontà negoziale (contrattuale o di negozio unilaterale come autorizzatorio tipico)⁶⁹, inclusa o meno in un più ampio schema di contratti/atti collegati⁷⁰, non esclude la necessità di manifestare l'autonomo consenso al trattamento. Rispetto a questa funzione e nei rapporti con il titolare, il consenso al trattamento dei dati è anche un atto negoziale (ad efficacia si voglia obbligatoria, dispositiva o derivativo-costitutiva)⁷¹, la cui manifestazione potrà desumersi dalla prestazione al consenso quale condizione di legittimità, o a nostro modo di vedere anche viceversa, ma che è logicamente autonomo dal primo e i cui requisiti possono essere potenzialmente difformi⁷².

69 La ricostruzione del consenso come manifestazione di volontà negoziale può, alternativamente, avvenire in termini di consenso contrattuale, valorizzando il contratto come modello prevalente di creazione della ricchezza in virtù della sua atipicità, ovvero di negozio autorizzatorio tipico (secondo la normativa speciale). L'adesione all'una o all'altra tesi si apprezza in termini di conseguenze giuridiche per la mancanza/difetto di consenso/autorizzazione (invalidità, inefficacia). M. TAMPONI, *Latto non autorizzato nell'amministrazione dei patrimoni altrui*, Milano, Giuffrè, 1992, p. 28 ss.

70 Sulla centralità dell'istituto del collegamento negoziale, nonostante l'autorevole tesi della rilevanza giuridica della nozione di operazione economica (da ultimo E. GABRIELLI, *L'operazione economica nella teoria del contratto*, in «Rivista trimestrale di diritto e procedura civile», 2009, p. 905 ss.), D. ACHILLE, *La funzione ermeneutica della causa concreta del contratto*, in Rin «Rivista trimestrale di diritto e procedura civile», 2017, p. 37 ss. spec. nnt. 73 – 75 e testo corrispondente.

71 Se è vero che gli attributi del consenso, ai fini della legittimità del trattamento, impediscono che esso possa essere desunto da altri comportamenti, non così è per l'eventuale desumibilità del consenso negoziale dal consenso prestatato per il trattamento o da altri atti dell'interessato-contraente. Lo speciale statuto del consenso per il trattamento sembra escludere che in concreto possano presentarsi ipotesi in cui, verificato il primo, manchino i requisiti del consenso negoziale, che è comunque integrato nella sua disciplina dalla normativa speciale. Si tratta, però, di due valutazioni autonome.

72 Si pensi all'ipotesi in cui il consenso del minore ultra sedicenne legittimi il trattamento ai dati personali (ex art. 7 GDPR), ma possa essere ritenuto non idoneo per la validità del contratto (che non può essere validamente concluso da un minore). Non è, infatti, univoco che la capacità di esercitare un diritto non patrimoniale includa quella di disporre dei correlati aspetti non patrimoniali. Per le opinioni dominanti sul punto, S. THOBANI, *op. cit.*, p. 106 ss.

Con riguardo, ad esempio, ai requisiti di della forma è ben possibile che le condizioni del consenso (negoziale/non negoziale) divergano, per cui si possa aver, in linea di principio, concesso/disposto in maniera valida del contenuto patrimoniale dei dati personali, ma con irregolarità ai fini della disciplina speciale e conseguenti sanzioni di tipo amministrativo, penale o anche di responsabilità civile⁷³, sebbene quest'ultimo piano tenderà a riverberarsi sul primo; ovvero, come nel caso del consenso del minore, che il consenso legittimamente prestato ai fini della liceità del trattamento, possa risultare inidoneo per difetto di capacità nell'operazione negoziale.

In ogni caso, il regolamento contrattuale o della complessiva operazione negoziale sarà integrato dall'applicazione dello statuto specifico connesso al trattamento dei dati personali, per la prevalenza degli aspetti connessi alla personalità dell'individuo, che esclude la stabilità degli effetti, come confermato dalla previsione del diritto di opposizione, esercitabile alle condizioni normative prescritte⁷⁴.

6. Consenso e studi comportamentali: critica alla rilevanza dell'informativa e del consenso nel processo di decision-making e per le finalità di protezione dei dati personali

Facendo riferimento al consenso in quanto base giuridica per il trattamento dei dati personali, si pone il problema di comprendere quale ne sia l'effettiva funzione, in altre parole, perchè il legislatore lo abbia previsto. Questa verifica delle ragioni e del ruolo effettivo

⁷³ In tal caso, infatti, la violazione della normativa per il trattamento dei dati personali (si pensi alla mancanza della forma scritta/consenso esplicito per i dati sensibili), si riverbera necessariamente sull'efficacia del contratto, in quanto *condicio iuris* di quest'ultimo. La mancanza, invero, di un requisito esplicito di consenso preventivo, infatti, esclude che l'antigiuridicità dell'attività di trattamento, in quanto priva di consenso, possa incidere sulla validità del contratto.

⁷⁴ La sovrapposizione tra consenso al contratto (profilo negoziale) e consenso autorizzatorio dell'autodeterminazione (ovvero condizione di legittimità del trattamento) è fenomeno già ampiamente investigato nell'ambito di consenso informato nella relazione terapeutica. In tema, V. CALDERAI, voce *Consenso informato*, in *Enc. dir.*, Annali VIII, 2015, p. 225 ss. spec. pp. 249-258; B. SALVATORE, *op. cit.*, p. 113 ss. Sul qualificazione del diritto di opposizione in termini di recesso e sulla revoca del consenso, S. MAZZAMUTO, *op. cit.*, p. 1034 ss.

del consenso (legittimante il trattamento) fa emergere le inevitabili connessioni e condizionamenti, già evidenziati, tra questo e la concreta operazione economico-negoziale nella quale s'inerisce⁷⁵.

La scelta di includere la volontà dell'interessato accanto ad altre "cause di liceità" del trattamento è significativa del ruolo che si è inteso attribuire al potere decisionale dell'individuo⁷⁶. In ambito europeo la configurazione della protezione dei dati quale libertà fondamentale ha fatto sì che tale potere assumesse il significato di libertà di autodeterminare la propria personalità rispetto alle informazioni disponibili collegandosi con il diritto all'autodeterminazione informativa⁷⁷. In questa prospettiva, la manifestazione di volontà, per essere libera, deve essere informata⁷⁸.

Una prima funzione che può attribuirsi al consenso informato è, quindi, quella di iniziale strumento di controllo della persona su aspetti connessi alla propria personalità tramite i "propri" dati: è l'individuo a decidere se, per quali dati e per (quali del)le finalità proposte fornire il proprio consenso. Ovviamente, – secondo uno schema ideale – la decisione consapevole presuppone la lettura dell'"informativa" che rende edotto l'interessato delle finalità del trattamento, di chi lo effettua e dei soggetti cui potersi rivolgere, dei propri diritti anche successivi alla prestazione del consenso al trattamento. L'informativa serve a bilanciare le asimmetrie informative, a far conoscere all'interessato i propri diritti e per quali finalità verranno utilizzati i dati a lui relativi, al fine della formazione

75 V. *supra* par. 4.

76 S. PATTI, *Consenso*, sub art. 23), p. 543.

77 Secondo nell'art. 6 della Dichiarazione dei diritti di Internet (disponibile al sito www.camera.it) in base al diritto all'autodeterminazione informativa, che non comprende il diritto al consenso: «Ogni persona ha diritto di accedere ai propri dati, quale che sia il soggetto che li detiene e il luogo dove sono conservati, per chiederne l'integrazione, la rettifica, la cancellazione secondo le modalità previste dalla legge. Ogni persona ha diritto di conoscere le modalità tecniche di trattamento dei dati che la riguardano. La raccolta e la conservazione dei dati devono essere limitate al tempo necessario, rispettando in ogni caso i principi di finalità e di proporzionalità e il diritto all'autodeterminazione della persona interessata».

78 Tuttavia, ad uguale risultato potrebbe arriversi adottando la logica proprietaria (o *commodification*) sui dati personali. V. nt. successiva.

di una scelta consapevole⁷⁹.

Se tale è l'obiettivo del legislatore, è facile sollevare in proposito il carattere di "vuota cerimonia"⁸⁰, proprio della sottoscrizione di qualsiasi formulario e che si celebra anche con riguardo al consenso informato in materia di *privacy*, e probabilmente in maniera accentuata. Infatti, qui, in aggiunta al generale e acclarato disinteresse per la lettura di "informativa" o "condizioni generali" da parte del destinatario delle stesse, l'oggetto stesso dell'informativa fornita (relativa ai dati personali) tende ad essere percepita dall'interessato come estranea all'operazione o al servizio e comunque non centrale nel momento in cui si è chiamati a concludere la transazione od operazione. Come la prassi facilmente evidenzia, la lettura dell'informativa *privacy* e l'eventuale consenso prestato tendono ad essere solo un passaggio (aggiuntivo e spesso fastidioso) rispetto all'ottenimento del bene o servizio cui il trattamento dei dati personali è funzionale. E allora, come nel caso di altre ipotesi di espressione di consenso che segue un'informativa obbligatoria, sarebbe facile rilevare dubbi in merito alla scelta normativa.

In via correttiva rispetto a questa prima interpretazione, secondo cui il consenso informato sarebbe funzionale a determinare scelte consapevoli in materia di *privacy*, è stato acutamente sottolineato come l'informativa propedeutica al consenso in questo caso assuma il ruolo non tanto di colmare asimmetrie informative nel rapporto tra due soggetti, quanto di avviare il controllo dell'interessato sul procedimento in cui si concreta l'attività di trattamento⁸¹. Ciò appare confermato dal fatto che l'obbligo di

79 L'accentuazione e la formalizzazione dell'informazione quale preciso obbligo preliminare alla manifestazione di volontà richiama l'indirizzo di politica legislativa che vede nel riequilibrio dell'asimmetria informativa il criterio ottimale per l'allocazione delle risorse, e quindi per le scelte individuali. È evidente il parallelismo con la gran parte della normativa delle contrattazioni (asimmetriche) nel mercato unico. Tale coincidenza di indirizzo politico appare ancora più evidente nel sistema statunitense, che pure adotta una legislazione per molti aspetti meno incisiva e meno organica, ove la disciplina della *privacy* costituisce aspetto della protezione del consumatore, su cui vigila infatti la *Federal Trade Commission*. Sulle fonti e sulla differenza di approccio, L. MIGLIETTI, *Il diritto alla privacy nell'esperienza giuridica statunitense ed europea*, Napoli, Edizioni scientifiche italiane, 2014, p. 39 ss. e L. MERLA, *Droni, privacy e la tutela dei dati personali*, in «Informatica e diritto», 2016, p. 29.

80 S. PATTI, *Consenso*, sub art. 23), cit., p. 541 ss.

81 S. MAZZAMUTO, *Il principio del consenso e il potere della revoca*, cit. spec. 998 e 1004. Assumendo l'assenza di alcun rapporto patrimoniale, rispetto al quale l'informazione può intervenire per una migliore allocazione delle risorse, l'a. vede l'informativa come primo atto del procedimento in cui si sostanzia l'attività di trattamento e che serve a dotare l'interessato degli strumenti per esercitare poteri di autotutela e controllo sul procedimento stesso.

fornire l'informativa sussista anche quando un successivo consenso non debba essere prestato, salvi alcuni casi⁸². L'informativa richiama l'attenzione sui poteri che poi spetteranno all'interessato nel corso del trattamento, ove questo trattamento non possa diversamente giustificarsi, non solo a fargli comprendere su cosa è chiamato ad esprimere il suo consenso⁸³.

Quest'osservazione sembra confermare l'idea che il trattamento non riguardi beni, né un problema di allocazione di risorse, come dimostrato dal fatto che non sorga alcun rapporto contrattuale tra interessato e titolare, ma allo stesso tempo non aggiunge nuovi spunti circa la funzione del consenso, se non provare ad ipotizzarsi che, stante la centralità dell'informativa, il consenso sia esso stesso un incentivo alla lettura dell'informativa.

In ogni caso, resta il dubbio già avanzato che né l'informazione né il consenso siano congegni che idonei ad agevolare il controllo dell'interessato sui fornitori⁸⁴.

Di conseguenza resta da chiedersi se, individuata la *ratio* del consenso informato, esso costituisca uno strumento efficace rispetto all'interesse che s'intende proteggere, vale a dire verificare l'*efficacia della normativa* o *effettività della tutela*⁸⁵.

Con *efficacia della normativa* (ove il sostantivo è utilizzato nel suo significato generale e non tecnico giuridico) si intende far riferimento alla verifica, attraverso criteri e strumenti d'indagine ricavabili anche da altre discipline (non solo economiche) o da studi empirici, della capacità delle norme giuridiche di realizzare gli scopi che si prefiggono. Il termine *effettività*, implica, invece, più specificamente la misura del grado di corrispondenza dei mezzi di tutela agli interessi tutelati, utilizzando i medesimi criteri di

82 Sulla somministrazione successiva dell'informativa, v. art. 13, co. 4, cod. privacy e art. 14 GDPR.

83 S. MAZZAMUTO, *op. cit.*, p. 1004 s.

84 A ciò si aggiunga che nella congerie di trattamenti cui si è esposti è ragionevolmente difficile ipotizzare una diffusa possibilità per il singolo di rintracciare a quale consenso possa risalire il trattamento di dati oggetto di ripensamento (ad esempio, in conseguenza di qualche evento sgradevole se non dannoso).

85 Una tale prospettiva, che si pone in una dimensione critica di valutazione delle regole esistenti anche per la loro interpretazione o modifica, deve, peraltro, tener conto non della idoneità in astratto alla realizzazione dell'obiettivo, ma dell'attitudine in concreto, tenendo cioè in considerazione le modalità di richiesta di consenso, che non possono prescindere dall'ambiente digitale.

valutazione. Poste queste minimali differenze, le due espressioni possono essere utilizzate come sinonimi.

Ciò detto, si è precedentemente riscontrato come l'interesse tutelato dalla previsione di un consenso informato particolarmente qualificato sia l'esercizio dell'autodeterminazione del singolo rispetto al diritto fondamentale alla protezione dei dati personali ed eventualmente, in aggiunta, l'incentivo al controllo successivo.

Va ora verificato se lo strumento del consenso informato sia in grado di assicurare la realizzazione di tale interesse⁸⁶.

Questa verifica può essere fatta utilizzando strumenti di analisi empirica e interdisciplinare che consentono di misurare i livelli di attenzione e consapevolezza della prestazione del consenso. Si tratta di approcci ben noti e propri degli studi comportamentali, di psicologia della decisione, che, nella parte in cui possono essere serventi alla riflessione giuridica, sono stati finora fatti propri dall'analisi economica del diritto, ad esempio in ambito di tutela del consumatore, principalmente da parte della letteratura straniera.

In proposito, chi scrive segnala che altri metodi di analisi interdisciplinare della ricerca giuridica con la sperimentazione comportamentale e gli studi psicologici sono stati intrapresi anche, di recente, da gruppi di ricerca in ambiente italiano. Si tratta di studi, ancora in fase di elaborazione, da cui originano le presenti riflessioni che saranno meglio espresse in successivi lavori⁸⁷.

86 La reale effettività del consenso quale diritto che tuteli l'interessato è stata già messa in dubbio, autorevolmente, da S. RODOTÀ, *Protezione dei dati personali e circolazione delle informazioni*, in *Riv. crit. dir. priv.*, 1984, p. 732 ss.; C. CAMARDI, *Mercato delle informazioni e privacy – riflessioni generali sulla l. 675/1996*, in «Europa e diritto privato», 1998, p. 1061. In senso convergente a quanto sopra nel testo, POPOLI, *Social Network*, cit. testo corrispondente e successivo a nt. 41, ove si riportano i risultati di un'indagine condotta nel 2010, che pur mostrando con riguardo all'utilizzo dei *social network* la tendenza delle più giovani fasce detà a cambiare le impostazioni *privacy* dei propri *account* (indice ciò di una possibile presa di consapevolezza in merito alle questioni connesse alla *privacy*), appaiono poi posti nel nulla dalla crescente complessità e lunghezza delle *privacy policy* e dalla frequenza del loro cambiamento, tale che «l'utente dovrebbe costantemente modificare le proprie impostazioni della *privacy* per mantenere il medesimo livello di *privacy* prescelto» (testo corrispondente a nt. 44).

87 Con specifico riguardo al consenso al trattamento, un esperimento di analisi comportamentale, con valutazione dei risultati in ambito giuridico, è stato condotto di recente, su commissione di un importante partner tecnologico, presso l'Università Suor Orsola Benincasa. Il progetto *Privacy and the Internet of Things: a behavioural and legal approach* ha realizzato un esperimento su un campione di soggetti volontari, richiesti di eseguire alcuni task (indicati dal soggetto committente) in relazione

Se si guarda, tuttavia, allo stato dell'arte degli studi comportamentali in tema di prestazione del consenso al trattamento dei dati personali, è stato ampiamente dimostrato il basso tasso di lettura delle informative nonché i notevoli ostacoli cognitivi che si riflettono sulla prestazione del consenso informato, in particolare in materia di protezione dei dati personali⁸⁸. Tali studi dimostrano come le decisioni assunte anche in materia di *privacy* non solo si sottraggono in astratto al paradigma della scelta razionale, com'è noto per gran parte dell'agire economico, ma che non costituiscono scelte consapevoli. Così anche nell'ipotesi in cui abbiano precedentemente affermato di desiderare un alto grado di tutela della propria *privacy*, gli interessati prestano il consenso per "scambiare" i propri dati anche con un minimo vantaggio o ricompensa⁸⁹. Le

ad attività di prestazione del consenso al trattamento dei dati, di navigazione in Internet e di utilizzo di applicazioni e software in ambiente digitale, al fine di valutarne il comportamento. La percezione e consapevolezza del singolo utente in relazione a quanto eseguito è stata valutata, tramite questionari e tecnologie di misurazione del comportamento (del movimento oculare), da esperti psicologi e statistici che valutano il livello cognitivo raggiunto dagli *users*, operando nel sistema operativo Windows 10. Tenendo conto delle evidenziate criticità sulla prestazione del consenso poste in luce dall'analisi psicologico-statistica, la parte di analisi giuridica del progetto si è interfacciata con quella dedicata all'usabilità, al fine di promuovere modifiche nelle modalità di richiesta del consenso ma anche normative. In proposito, ci sia consentito reinviare a L. GATT, R. MONTANARI e I. A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Politica del diritto*, 2017, p. 339 ss.

88 L'interazione con gli studi comportamentali, già ben nota in altri settori, e che seleziona i meccanismi di causazione delle decisioni, ha come fine ultimo quello di migliorare la capacità del diritto di regolare i comportamenti e a superare, indicando «un anacronismo della regolamentazione giuridica». Vedi O. JONES e TH. GOLDSMITH, *Diritto e biologia comportamentale*, in *i-lex*, 2006, 27 ss., spec. 30; B. LURGER, *Empiricism and Private Law: Behavioral Research as Part of a Legal-Empirical Governance Analysis and a Form of New Legal Realism*, in «Austrian Law Journal», 2014, p. 20 ss. In generale, sull'*antirealismo* su cui si basa il modello normativo dell'informazione e quindi della *scelta razionale*, nei rapporti del consumatore, si veda R. CATERINA, *Psicologia della decisione e tutela del consumatore*, in «Analisi giuridica dell'economia», 2012, p. 67.

89 A. ACQUISTI, *Privacy*, in *Riv. pol. econ.*, 2005, p. 319; A. ACQUISTI e J. GROSSKLAGS, *What Behavioral Economics Teach Us About Privacy?*, in *Digital Privacy: Theory, Technologies and Practices*, a cura di A. Acquisti e altri, Auerbach Publications, 2007, p. 367 ss.; D. J. SOLOVE, *Privacy self-management and the Consent Dilemma* 126 *Harv. Law Rev.* 1880 (2013); F. Z. BORGESIU, *Informed consent: We Can Do Better to Defend Privacy*, IEE, 2015 (Vol. 13, p. 103 - 107) – recommended cit.; ID. *Behavioural Sciences and the Regulation of Privacy on the Internet*, Amsterd. Law School Research Paper no. 2014 – 54; O. BENSHAHAR e A. CHILTON, *Simplification of Privacy Disclosure: An Experimental Test*, 45 *Journ. Legal Studies* (S2): S41-S67 (2015); S. BAROCAS e H. NISEMBAUM, *On Notice: the Trouble with Notice and Consent*, *Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information*, October 2009. Available at SSRN: <https://ssrn.com/abstract=256740>

evidenze empiriche indicano come, in aggiunta a una non ben chiara percezione del significato e della portata della *privacy* nella coscienza sociale, il consenso al trattamento dei propri dati personali si formi per via di euristiche o altre scorciatoie cognitive che non dipendono dal modo in cui l'informativa è presentata o il consenso è richiesto⁹⁰. Può così avvenire che la decisione sul trattamento sia condizionata dalla generale percezione dell'individuo circa le sue capacità di controllo in un determinato momento (*control paradox*) o dal tipo di servizio cui l'informativa accede, e, in generale, dall'incapacità della mente umana di valutare compiutamente tutti i costi e benefici di una determinata azione (*razionalità limitata*).

Tale razionalità limitata dell'individuo si amplifica quando oggetto della decisione è il trattamento dei propri dati personali. Con riguardo ai dati personali, infatti, il carattere astratto del concetto di trattamento e delle sue conseguenze rendono questi ultimi, in via di principio, oggetto di non facile comunicazione e spiegazione. Né l'informativa obbligatoria ha per oggetto le conseguenze negative derivanti dal trattamento. Quand'anche ciò avvenisse (si pensi ad esempio ad un'informativa che provi a spiegare i vantaggi e gli svantaggi della profilazione o degli utilizzi dei dati da terze parti) tali conseguenze sarebbero difficilmente traducibili in immagini o frasi minime (si pensi, per differenza, all'impatto emotivo delle immagini o frasi prescritti ai produttori di tabacco). L'impatto – eventualmente negativo – del trattamento, infatti, si misura sul lungo termine, mentre si colloca sul breve periodo il beneficio che deriva dal trattamento, come avviene nel caso di servizi offerti “gratuitamente” ma,

90 Le riflessioni offerte nel testo mirano a dimostrare l'inefficacia della normativa rispetto alla *ratio* di tutela e a suggerire una riflessione che sia calibrata sulle capacità cognitive dell'uomo medio, al fine di conformare la normativa su ciò che si può realisticamente pretendere. L'elemento connaturato dell'irrazionalità dell'individuo di per sé stessa non può costituire elemento atto a menomare la corretta formazione della volontà, per lo meno nella tradizionale prospettiva dei vizi o delle incapacità, che sono – per via del requisito della libertà del consenso – applicabili anche al consenso al trattamento. L'opposta visione consistente nel dare rilievo alle connotazioni psicologiche che caratterizzano la comune percezione cognitiva della persona al fine di minare la libera prestazione del consenso indurrebbe al risultato per cui tutti i consensi sarebbero viziati o in ogni caso deresponsabilizzare gli individui, premiando i più sprovveduti. In proposito anche R. CATERINA, *op. cit.*, p. 81 nonché U. MORERA ed E. MARCHISIO, *Finanza, mercati, clienti e regole ... ma soprattutto persone*, in «Analisi giuridica dell'economia», 2012, p. 19 ss.

nella complessiva operazione economica, in cambio dei dati personali⁹¹. Ciò tenderà a far propendere la scelta sull'immediato beneficio (*miopia* nell'analisi comportamentale)⁹².

Vi è, infine, un ulteriore dato che induce a ritenere la prestazione del consenso al trattamento non significativa ed è rappresentato dal carattere routinario dei consensi, richiesti e forniti, in consanguenza della diffusione di attività di trattamento, anche in ambiente digitale, che abbassa ancor più il livello di attenzione delle persone fisiche, costantemente richieste di cliccare su qualche opzione di consenso.

È quanto mai dubbio allora che il consenso possa rappresentare un meccanismo avente una qualche funzione di scelta consapevole per la protezione del diritto del singolo ai suoi dati personali. Tali considerazioni reclamano una certa attenzione da parte dell'interprete e del legislatore.

Anche con riguardo alla funzione del consenso informato quale fondamento di un ben più articolato procedimento di controllo del trattamento e quindi alla possibile *ratio* di strumento per sollecitare l'attenzione da parte dell'interessato, valgono le considerazioni sopra svolte sulle capacità cognitive della persona al momento della somministrazione dell'informativa.

Le soluzioni a tale pur nota aporia che intanto hanno fornito il legislatore – come si è visto – e in ambito italiano, l'Autorità di settore, sono state rappresentate dalla prescrizione di sempre più articolate qualificazioni del consenso unite alla semplificazione e potenziamento della trasparenza dell'informativa⁹³.

91 D. J. SOLOVE, *op. cit.*, p. 1891.

92 Sul paradosso del controllo, la "lungimiranza limitata" e altre scorciatoie cognitive A. ACQUISTI, *Privacy*, cit., p. 357 e *passim* anche per ulteriore bibliografia. Un esempio di comportamenti simili è nell'acquisto di beni che diano un piacere immediato (dovuti o meno a dipendenza) come nell'acquisto di tabacco o altro, nonostante l'informativa sempre più aggressiva e realistica che la normativa impone, ovvero nella mancata predisposizione di piani pensionistici, in un sistema a carattere contributivo o simile.

93 Quale espressione della normativa nazionale ancora applicabile, è da registrare in proposito un discreto numero di provvedimenti dell'Autorità italiana in tema di sanzioni per l'informativa non somministrata o scorretta, tra cui anche – di recente – richieste di adeguamenti da parte di imprese extra-UE, come nel ben noto caso Google. L'azienda americana ha accettato di conformarsi alle prescrizioni mosse dal Garante italiano nel 2013 in relazione all'informativa fornita: miglioramento e differenziazione della *privacy policy* in relazione ai diversi servizi forniti, consenso *ex ante* per finalità di profilazione, archiviazione e cancellazione dei dati. Maggiori dettagli sono disponibili

Tuttavia, è stato altresì dimostrato come un'adesione sempre più stringente ai requisiti normativi, o il "miglioramento" dell'informativa non sia realmente in grado di incidere sulla consapevolezza dell'utente⁹⁴.

Ci sembra evidente che se si resta nella logica della informativa o dei suoi progressivi, minimali miglioramenti, il rischio è di rimanere all'interno di un labirinto che non porta a risultati significativi.

Peraltro, la prestazione *ex ante* del consenso qualificato al trattamento, al di là di rappresentare, quale simulacro, l'idea dell'autodeterminazione del singolo sulle informazioni a lui relative conformemente al modello teorico dei diritti fondamentali, non è in grado di limitare i rischi di una diffusione o di una costruzione dei dati, anche per la complessità di governo del mercato degli stessi. Molti dei rischi per la protezione dei dati sono connessi alla profilazione o, in ogni caso, all'aggregazione dei dati da parte di più soggetti nel tempo ed è impossibile per l'individuo prevedere al momento della isolata prestazione del consenso i costi e i benefici del trattamento.

Prova ne è che lo stato attuale della sorveglianza e della tecnologia non consente in ogni caso di evitare invasioni della sfera privata (si pensi al fenomeno dello *spamming*). Ciò è vero, come l'esperienza insegna, con riguardo anche al caso di utente, singolarmente e particolarmente, accorto nel prestare il consenso al trattamento dei propri dati, anche e non soltanto per i rischi di profilazione⁹⁵.

al link <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3740038>
Complessivamente, il numero di provvedimenti dell'Autorità in materia di informativa (artt. 13 e 161 cod. privacy) sono 642 (fonte: sito GarantePrivacy)

94 Le tecniche di informativa multi-livello o l'utilizzo di siti comparativi delle informative privacy (es. EULalyzer) non sembrano aver determinato significative modifiche nei comportamenti o stimolato una migliore consapevolezza sul tema. Sul punto, O. BENSHAHAR e A. CHILTON, *op. cit.* ove si dimostra, sulla base di un articolato esperimento, come nessuna delle tecniche adottate di semplificazione dell'informativa tramite *best practices* o *warnings* abbia modificato il comportamento degli "interessati"; L. J. STRAHILEVITZ e M. B. KUGLER, *Is Privacy Policy Irrelevant to Consumers?* 45 *Journ. Legal Studies* S2, pp. S69-S95 (2017) hanno condotto un altro esperimento su più di 1000 americani sottoponendo loro (a caso) due versioni testi di informative privacy di Google e Facebook, una chiara l'altra vaga, per autorizzare il riconoscimento facciale e il trattamento dei relativi dati. I risultati dell'esperimento confermano che le scelte degli utenti, che pure ritenevano quel tipo di trattamento trattamento altamente intrusivo, non siano cambiate in ragione del linguaggio dell'informativa, ma delle norme sociali e dell'esperienza tecnologica.

95 Nel 2010 si stima che il 90% delle e-mail non siano state altro che *spam*. M. BOCCHIOLA, *Privacy. Filosofia e politica di un concetto inesistente*, Roma, Luiss University Press, 2014, p. 46.

Ritorna allora, per questa via, il riferimento alla realtà complessa della circolazione dei dati, alle loro regole tecniche di funzionamento, al mondo dei *big data*, fenomeni che rendono tali dati difficilmente controllabili dal consenso del singolo né facilmente tracciabili per l'interessato in un momento successivo⁹⁶.

7. I rimedi privatistici: il problema del risarcimento del danno

Per quanto sommariamente esposto, a nostro modo di vedere, l'autodeterminazione dell'interessato, per i connaturati difetti cognitivi di questi, non ha *in nuce* possibilità di esplicitarsi, né il numero di attività di trattamento dei dati personali può ricevere significative variazioni dall'allocazione del potere di scelta sull'individuo-persona fisica⁹⁷.

Il diritto alla protezione dei dati personali, rispetto al quale il consenso è funzionale, sconta, per altro, un'ulteriore criticità: la difficoltà di essere tutelato *ex post*, in sede *civilistica*, autonomamente, cioè ove non siano stati lesi significativamente altri beni giuridici (ad es. riservatezza, reputazione, identità). Quest'ostacolo che la giurisprudenza individua nella mancanza di "gravità della lesione" e "serietà del danno" tale da escludere il risarcimento, riporta al problema della natura stessa di tale diritto, come più avanti si vedrà.

La (quasi) oggettivizzazione della tutela del danno da trattamento dei dati personali, prevista nell'ordinamento italiano e sostanzialmente confermata dal Regolamento europeo⁹⁸, mentre ha favorito il danneggiato

96 Art. 5, §1, lett. b) GDPR e art. 11, co. 1, lett. b) cod. privacy. Sulla inappropriatezza di approcci ancora individualistici e sulla necessità di una soluzione olistica, che non fondi la protezione dei dati sulla mera sommatoria della tutela e regolarità dei comportamenti relativi ai singoli trattamenti, v. S. Y. ESAYAS, *The idea of 'emergent properties' in data privacy: towards a holistic approach* 25 *Int. Journ. Law & Info. Technology*, 139, 2017.

97 D. J. SOLOVE, *op. cit.*, p. 1898 ss.

98 La risarcibilità del danno per effetto del trattamento di dati personali secondo lo schema dell'art. 2050, nonché la risarcibilità del danno non patrimoniale, in violazione delle regole per il trattamento (art. 15 cod. privacy) ricevono una sostanziale conferma dal nuovo tenore dell'art. 82 GDPR, nonostante alcune diversità, relative all'individuazione dei soggetti responsabili (il titolare e responsabile in luogo del "chiunque") e alla prova liberatoria (non imputabilità in luogo della prova di aver adottato tutte le misure idonee, secondo l'art. 2050). Se nel primo caso ne deriva la chiara ascrizione alla responsabilità per colpa per i soggetti diversi da quelli coinvolti

sotto il profilo dell'antigiuridicità e del criterio di imputazione, non ha invece inciso sui criteri generali per determinare l'ingiustizia del danno⁹⁹, ed in particolare sulla cd. serietà del danno. Ciò ha inciso sulla risarcibilità del danno non patrimoniale in caso di illecito trattamento dei dati personali¹⁰⁰.

Un'analisi della, invero scarna, giurisprudenza relativa al rimedio risarcitorio previsto dalla legislazione speciale¹⁰¹ evidenzia come la violazione delle norme relative al trattamento dati personali (comprendenti anche quelle sul consenso), non comporti spesso la disponibilità del rimedio risarcitorio in capo alla persona fisica, per l'assenza di danno¹⁰² – ovvero per il carattere bagattellare dello stesso (si

direttamente nell'attività di trattamento appare una disposizione opportuna, alcuni dubbi possono sorgere in merito alla potenziale attenuazione del contenuto delle cause di esclusione della colpevolezza, che tuttavia si potrebbero essere risolti in via interpretativa, potendo adeguare la nuova esimente soggettiva.

99 F. DI CIOMMO, *Vecchio e nuovo in materia di danno non patrimoniale da trattamento dei dati personali*, in «Danno e responsabilità», 2004. p. 820 ss. e E. BARGELLI, sub art. 15, co. 2, in *La protezione dei dati personali. Commentario*, a cura di C.M. Bianca e F. D. Busnelli, t. I, Padova, Cedam, 2007, p. 410 ss., spec. p. 420. Sulla responsabilità civile da trattamento dei dati v. G. COMANDÈ, sub art. 15, co. 1, in *La protezione dei dati personali. Commentario*, a cura di C.M. Bianca e F. D. Busnelli, t. I, Padova, Cedam, 2007, p. 362 e con riguardo alla normativa pre-vigente E. NAVARRETA, sub art. 29, co. 9, in *Tutela della privacy*, a cura di C.M. Bianca e F. D. Busnelli, «Nuove leggi civili commentate», 1999, p. 690 ss.

100 Sul risarcimento da illecito trattamento, F. D. BUSNELLI, *Il "trattamento dei dati personali" nella vicenda dei diritti della persona: la tutela risarcitoria*, in *Trattamento dei dati e tutela della persona*, a cura di V. Cuffaro, V. Ricciuto, V. Zeno-Zencovich, Milano, Giuffrè, 1998, p. 181 ss.

101 Una ricerca giurisprudenziale condotta sulla banca dati *DeJure* (nel giugno 2016) ha prodotto un risultato di 115 provvedimenti in materia di violazioni dell'art. 15 d. lgs. 196/2003. Già negli anni immediatamente successivi il 2003, a commento della relativa disposizione, veniva rilevata la scarsità di decisioni giudiziali (si veda G. COMANDÈ, *op. cit.*, p. 369).

102 Il danno patrimoniale da illecito trattamento dei dati personali trova più facile ingresso, come nell'ipotesi di illegittimo trattamento di credenziali bancarie/finanziarie, o di *phishing* (da ult. Cass. civ., sez. I, 23.05.2016, n. 10638, in *DeJure*). Nell'ambito delle informazioni sulle relazioni creditizie, si pensi al caso della comunicazione di dati finanziari del singolo, che portino alla mancata stipulazione di un contratto. In tali ipotesi, se il rimedio *lato sensu* amministrativo (provvedimento del Garante) può impedire all'impresa commerciale di trattare dati raccolti, per determinate finalità dai Sistemi di informazione creditizia, più difficile appare la provadel danno per la mancata stipula del contratto. In proposito si vedano i provvedimenti del Garante - 4 maggio 2006- Crif S.p.A. [doc. web n. 1302311; Experian Information Services S.p.A. [doc. web n. 1302326]; H3G S.p.A. [doc. web n. 1302339]; Telecom Italia S.p.A. [doc. web n. 1302373]; Vodafone Omnitel N.V. [doc. web n. 1302385]; Wind telecomunicazioni S.p.A. [doc. web n. 1302395]. A tal proposito, la circolazione delle informazioni economiche (Codice deontologico centrali rischi private, che prevede quali informazioni di "cattivo pagatore" o debitore moroso possano essere comunicate ai fini dell'emissione di un finanziamento) è consentita dall'attuale art. 24, *lett. d)* cod. privacy – dati relativi allo svolgimento di attività economiche

pensi allo *spamming*), o infine per la difficoltà di rintracciare il titolare o responsabile del trattamento (potrebbe darsi il caso di una profilazione non autorizzata che conduca ad una diffusione di gusti personali del singolo che egli intende mantenere riservati).

Le principali questioni si pongono nei casi in cui venga in discussione la lesione di un interesse non patrimoniale in conseguenza della violazione dei dati personali, in merito alla configurabilità e liquidazione del danno. La mancata prova del danno o della sua serietà (cioè il pregiudizio concretamente patito) sono la principale causa del rigetto delle domande risarcitorie¹⁰³. La lesione di una libertà fondamentale come il diritto alla protezione dei propri dati sconta, quindi innanzitutto, una difficoltà di prova e di liquidazione (anche se necessariamente equitativa) che è comune ai danni non patrimoniali diversi dal biologico¹⁰⁴. Vi è, tuttavia, anche la difficoltà di accertare una lesione seria in caso di

e 6 cod. deontologico centrali rischi, per le informazioni negative). Sul punto, il GDPR interviene in via preventiva prevedendo che le decisioni che producono effetti giuridici (concessioni di prestiti etc.) non possono essere basate su trattamento automatizzato di dati (profilazione) (art. 22 e cons 71).

103 Cass., 15 luglio 2014, n. 16113, in *Danno resp.*, p. 339 ss., con commento di V. CECCARELLI, cui è conforme Cass., 11 gennaio 2016, n. 222 in *DeJure*, con nota di Alovio, in *Risarcimento del danno per diffusione indebita di dati sanitari*, in «Diritto e Giustizia», 2016, p. 3, che confermando l'inconfigurabilità del danno-evento, chiarisce che la lesione del diritto alla protezione dei dati personali deve superare la soglia minima di tollerabilità imposta dai doveri di solidarietà secondo il bilanciamento con il principio di solidarietà previsto dall' art. 2 della Costituzione, che prevede che il riconoscimento e la garanzia dei diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale. Una lesione del diritto alla *privacy* si può verificare pertanto solo nel caso di offesa sensibile della portata effettiva del diritto. In senso analogo, anche in materia di dati cd. supersensibili (rettificazione del sesso), Cass. 13 maggio 2015, 9785 in *Fam dir.*, 2016, p. 469 ss., e sensibili, Cass., 19 maggio 2004, n. 10947, in *Fam. dir.*, 2016, p. 468. Tale orientamento non è sempre seguito nella giurisprudenza di merito. Sul punto V. CECCARELLI, *La soglia di risarcibilità del danno non patrimoniale da illecito trattamento dei dati personali*, in *Danno e resp.*, cit., p. 348.

104 Con riguardo alla quantificazione del diritto alla riservatezza per violazione dell'art. 15 cod. privacy, nel quadro della grande incertezza sulla valutazione del pregiudizio non patrimoniale, Trib. Milano, 3 settembre 2012 in *Riv. it. medicina legale*, 2013, p.1067 con nota di Serani; Appello Milano, 22 luglio 2015, in *Danno e resp.*, 2015, p. 1047, con note di G. PONZANELLI, *Quanto vale la riservatezza di un giocatore di calcio?*, p. 1057 e di R. FOFFA, *Il caso Vieri: secondo tempo*, *ibid.*, p. 1059. Con specifico riguardo all'illecito trattamento dei dati personali e all'ammissibilità della prova presuntiva anche dell'esistenza del danno dall'accertamento amministrativo dell'illiceità da parte del Garante, si veda Cass., 15 ottobre 2015, n. 20890 in «Danno e responsabilità», 2016, p. 372, con commento di M. GAGLIARDI, *La prova del danno non patrimoniale in caso di trattamento illecito dei dati personali*, p. 373 ss.

violazione di illecito trattamento dei dati, in particolare ove a tale illiceità non si accompagni la lesione della riservatezza o di altro diritto della personalità¹⁰⁵. Posta la necessità, secondo la teoria dell'illecito civile, che all'antigiuridicità della condotta si affianchi la necessità dell'accertamento del danno ingiusto, può dirsi che con riguardo all'illecito trattamento dei dati l'ingiustizia del danno acquista una dimensione "esterna" venendo la serietà della lesione e la gravità del danno (secondo l'endiadi cara alla giurisprudenza)¹⁰⁶ di regola vagliate e misurate su beni differenti dalla protezione del dato personale in sé.

Si tratta, a ben vedere, dell'obiezione sollevata già a partire dalla dir. cd. madre in tema di risarcibilità del danno da illecito trattamento secondo cui la lesione del diritto alla protezione dei dati personali potesse essere risarcibile solo se dall'illecito trattamento fosse derivata la lesione di ulteriori diritti (onore, reputazione, identità personale e così via), ovvero tale diritto assumesse non solo autonomo rilievo a rango di "diritto primario" (come poi confermato dall'art. 8 della Carta Nizza, dall'art. 4 cod. privacy ed ex art. 2 Cost.), finanche poi essendo tutelabile *in re ipsa*¹⁰⁷.

Non può oggi negarsi la formalizzazione del diritto alla protezione dei dati personali come libertà fondamentale, e diritto autonomo, tale da fondare l'ingiustizia del danno. Tuttavia, esclusa la configurabilità nell'attuale sistema italiano di un danno *in re ipsa*, tale formalizzazione non consente di tralasciare il dato strutturale del diritto alla protezione dei dati personali rappresentato dalla funzionalizzazione alla salvaguardia di interessi essenziali della persona sottesi ai diritti della personalità,

105 Com'è chiaro in Cass., 19 luglio 2016, n. 14694 in *De Jure* ove la liquidazione equitativa è chiaramente riferita alla lesione della riservatezza e reputazione, ma il richiamo agli altri beni è presente in tutte le pronunce in materia. Va inoltre precisato che anche nelle due ipotesi rintracciate in cui la giurisprudenza tende a liquidare il mero "danno morale" derivante dalla illecita diffusione dei dati (Cass., 05 settembre 2014, n. 18812, in *De Jure*; Cass., 14 agosto 2014, n. 17974, in *De Jure*), può sollevarsi qualche critica in ordine ad una liquidazione operata sì in via equitativa, ma in assenza di dimostrazione, anche presuntiva, di un pregiudizio anche nella sfera non patrimoniale.

106 Cass., 15 luglio 2014, n. 16113, cit.; Cass., 11 gennaio 2016, n. 222, cit.

107 S. SICA, *Danno morale e legge sulla privacy informatica*, in *Danno resp.*, 1997, p. 283 ss. Con riguardo al trattamento dei dati, il dibattito, in dottrina, sulla questione, è ripreso sinteticamente da S. THOBANI, *op. cit.*, p. 97 ss.

come in primo luogo il diritto al rispetto della vita privata¹⁰⁸. In tal senso, l'esperienza giurisprudenziale tende a dimostrare come la concreta risarcibilità, *via* stavolta la serietà del danno sofferto, passi di regola per le lesioni di altre situazioni giuridiche. Le diverse argomentazioni che in progresso di tempo hanno sostenuto tale posizione evidenziano un nodo problematico di fondo.

Inoltre, la mancanza di autonomia di un diritto della personalità non è argomento nuovo. Sebbene sotto la diversa cifratura della configurabilità del danno esistenziale, si era già posto in passato con riguardo ad altri diritti della personalità¹⁰⁹, facendo emergere casi esemplificativi in cui la lesione del diritto, anche riguardante la persona, non necessariamente provoca riflessi che incidono sulla dimensione non patrimoniale. Situazione analoga, anche in una grammatica parzialmente differente, si pone con riguardo al trattamento dei dati personali.

Qui le difficoltà in tema di rimedio risarcitorio, correlate al carattere non rivale per quanto escludibile del dato stesso¹¹⁰, tendono a confermare, anche sul piano della tutela *ex post*, che dal diritto alla protezione dei dati in sé considerato non emerge nettamente il contenuto dell'interesse protetto per il privato, in una prospettiva di attualità del danno e quindi di chiara individuazione dell'interesse stesso.

Potrebbe allora pensarsi che la reale finalità di tutela del diritto a veder protetti i propri dati (non sensibili, la violazione dei quali porta più facilmente a violazioni di altri beni della persona), in quanto sfuggente dalla sfera del singolo, possa più efficacemente essere perseguita tramite meccanismi di regolazione dei mercati o di protezione di una più generale condizione dell'esistenza umana.

108 C.M. BIANCA, *Nota introduttiva*, in *La protezione dei dati personali. Commentario*, a cura di C.M. Bianca e F. D. Busnelli, t. I, Padova, Cedam, 2007, p. XXIII.

109 P. ZIVIZ, *Lesione del diritto all'immagine e risarcimento del danno*, in «Responsabilità civile e previdenza», 2000, p. 710 ss., in tema di danno all'immagine di persona non celebre.

110 V. VISCO COMANDINI, *Il ruolo della privacy nella competizione per l'accesso delle risorse pubblicitarie su Internet*, in «Diritto, economia e tecnologie della privacy», 2012, n. 1, p. 1 ss.

8. *L'alternativa: un mondo senza privacy?*

Quale possibile alternativa allo scenario appena descritto e analizzato?

All'estremo opposto di un sistema nel quale, dal punto di vista privatistico, la protezione dei dati appare non efficacemente disciplinata o non tutelabile, si potrebbero riproporre le più radicali teorie di tipo normativo, proprie dell'analisi economica liberista, le quali contestano la stessa ragion d'essere di una disciplina di tutela dei dati personali, e della stessa riservatezza. Tale disciplina è ritenuta idonea a porre solo un ostacolo ai flussi informativi, che invece rendono le scelte e i mercati più efficienti, consentendo l'incrocio ottimale tra domanda e offerta¹¹¹. L'idea che è alla base di tale proposta è, infatti, che la riservatezza non costituisca un valore (o bene giuridico), ma anzi che il celamento delle informazioni risponda a intenti manipolatori, e di conseguenza la protezione dei dati, anche di quelli sensibili, sia dannosa, poiché impedisce l'efficiente allocazione delle risorse¹¹². Il palesamento di questi ultimi consentirebbe invece l'emersione delle condotte discriminatorie e di espungere dal sistema gli attori di condotte inefficienti.

Ciò non esclude che vi possano essere settori che richiedano un regime di esclusiva sulle informazioni o che in un sistema in cui non sussistano strumenti di tutela delle informazioni, sulle stesse non si formi comunque un mercato.

In verità, la proposta avanzata dalla scuola liberista di analisi economica non esclude del tutto una regolamentazione della riservatezza o dei dati personali, che può essere efficiente (è il caso del *privacy tort*) o potenzialmente ininfluenza sul benessere sociale (con riguardo ad una disciplina che conferisca il diritto sull'informazione/dato personale in capo a colui cui esso si riferisce), ma esclude che vi

111 R.A. POSNER, *The Right of Privacy* 12 *Georgia Law Rev.* 393 (1977); ID., *Privacy, Surveillance, and Law* 75 *U. Chi. Law Rev.* 245 (2008). Per una sintesi efficace di alcuni aspetti in lingua italiana, G. PINO, *Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali*, in *Libera circolazione e protezione dei dati personali*, a cura di Rocco Panetta, t. I, Milano, Giuffrè, 2006, p. 259, spec. 277 ss.

112 R. E. EPSTEIN, *The Legal Regulation of Genetic Discrimination: Old Responses to New Technology*, 74 *B.U.L. Rev.* 1, 12 (1994).

sia una solida giustificazione economica al *right to privacy* e possano esservi limiti nel mercato delle informazioni¹¹³.

Peraltro, tale teoria economica tradizionale è stata oggetto di critiche. Un sistema che tenda alla *full disclosure*, o alla illimitata circolazione (ovvero un mercato non regolamentato dei dati personali) dei potrebbe rischiare di essere, parimenti inefficiente, generando scelte discriminatorie non sempre riconoscibili come tali, ovvero fondate su informazioni false (e non immediatamente smascherabili come tali)¹¹⁴; ovvero, infine, esternalità negative sugli interessati/utenti, per effetto dei danni derivanti dall'utilizzo da parte di terzi dei dati¹¹⁵. Inoltre, il pur attraente modello alternativo di un mondo senza *privacy* probabilmente manca di considerare alcuni aspetti probabilmente connaturati alla persona umana, relativamente alla riservatezza¹¹⁶, oltre al limite giuridico attuale rappresentato, in Europa, dalla configurazione come libertà fondamentale, anche se non in termini di prerogativa assoluta, del diritto alla protezione dei dati personali. La stessa teoria economica successiva ha posto in rilievo i limiti di tale approccio¹¹⁷.

Ciò che, a nostro modo di vedere, può essere tratto come utile spunto di riflessione dall'analisi economica della disciplina *privacy* (che è anche disciplina della protezione dei dati personali) è, invece, la traduzione dei meccanismi di tutela nella grammatica essenziale propria di tale approccio, che consente di inquadrare le scelte legislative secondo categorie più generali, le quali possono prestarsi, secondo passaggi concettuali ulteriori, anche a funzionalizzazioni diverse dall'accezione di benessere sociale proprio della teoria economica. Così, ad esempio, la valutazione del consenso secondo la categoria della *property rule*, del risarcimento, secondo quella della *liability rule*, di un sistema di limitazione del mercato (regola di invalidità dei trasferimenti dei dati) secondo quella della *inalienability*, riescono a fornire il quadro del

113 R.A. POSNER, *The Right of Privacy*, cit.

114 R. CALO, *Privacy and Markets. A Love Story* 91 *Notre dame Law rev*, 649 (2016).

115 Una sintesi è in I. COFONE, *The Dynamic Effect of Information Privacy Law* 18 *Minn. L. J. Sci. & Tech.* 517 (2017), spec. 528 s.

116 In tal senso, anche recenti analisi filosofiche, come M. BOCCHIOLA, *op. cit.*, p. 140 ss.

117 Si vedano aa. alle ntt. 113 e s. ove ulteriore bibliografia.

potenziale impatto ed efficacia delle norme, utili anche nell'ambito di analisi non economiche di tipo normativo¹¹⁸.

Dalla pur sintetica panoramica proposta può, infine, ricavarsi, anche alla luce delle proposte antitetiche fatte, la necessità di una disciplina di tutela dei dati, che tuttavia appare sempre più dover essere valutata in relazione agli interessi essenziali della persona, tra cui vi è quello di un necessario spazio vitale dell'individuo, connaturato alla stessa natura umana, i cui confini tuttavia possono essere meglio tracciati¹¹⁹.

9. Alcune proposte in uno scenario inefficiente e complesso

Come detto, la Carta dei diritti fondamentali UE individua il consenso quale uno soltanto dei possibili legittimi fondamenti previsti dalla legge al trattamento dei dati di carattere personale. La prestazione del consenso come regola non generale è confermata nell'ordinamento interno¹²⁰ e dalla normativa che troverà applicazione a partire dal 2018, la quale considera come legittimo interesse del titolare del trattamento, tale da escludere il previo consenso dell'interessato, ma in ossequio al bilanciamento degli interessi, anche la finalità di *marketing* diretto¹²¹. Tuttavia, il consenso mantiene il ruolo di architrave dei poteri di controllo ed intervento riconosciuti all'interessato sulle proprie informazioni volti a determinare la costruzione della propria sfera privata, i quali costituiscono la sostanza del diritto alla protezione dei dati personali.

118 In tal senso, I. COFONE, *The Dynamic Effect of Information Privacy Law*, cit., che giunge ad una proposta di scenario efficiente basato su una regola di consenso (*property rule*) a tutela degli usi dei dati "primari", cioè da parte dei titolari ai quali sia stato fornito il consenso, e su una regola di responsabilità oggettiva (*liability rule*) a tutela dell'utente per usi secondari fatti da soggetti terzi.

119 In una diversa prospettiva, L. STRAHILEVITZ, *Toward a Positive Theory of Privacy Law*, cit., pone il problema, rispetto alle politiche del diritto in materia di protezione dei dati, di identificare i gruppi di interesse che nei diversi ambiti vengono favoriti o meno da una scelta normativa.

120 Artt. 24, 43, 44 cod. privacy.

121 Tale previsione ci sembra possa capovolgere l'attuale lettura dell'art. 24 lett d) cod. privacy (trattamento di dati relativi allo svolgimento di attività economiche, per il quale non è richiesto il previo consenso) che riguarda i dati personali quali ragione sociale, numero partita IVA. Proprio in caso di marketing diretto è tuttavia sempre consentito il diritto di opporsi alla profilazione (art. 21 diritto di opposizione).

Si è dubitato, nelle riflessioni che precedono, che sia il consenso sia il potere di controllo siano strumenti in grado di realizzare tale sfera di autodeterminazione del singolo, soprattutto nell'attuale dimensione *online* della vita individuale. Anzi, potenzialmente la previsione di tali diritti tende ad ingenerare nel singolo la falsa convinzione del controllo e della protezione dei propri dati. In tal senso può condividersi il rilievo dei fautori del "paternalismo libertario", secondo cui l'illusione della scelta non sia meno paternalistica dei meccanismi ispirati a regole di *default* ovvero ad altre strategie di "spinta gentile"¹²². Per la stessa ragione, tuttavia, le politiche di *nudging* nei riguardi dell'interessato alla protezione dei dati personali non appaiono risolutive (attraverso, ad esempio, la sostituzione dell'*opting in* con l'*opting out*), nella prospettiva della ricerca di una protezione effettiva, che non può dipendere dall'interessato.

Potrebbe esservi allora spazio per un sistema in cui la prestazione del consenso non venga più richiesta, restando un residuo diritto al controllo sui propri dati, ove intercettati, trattati secondo regole procedurali ispirate a correttezza, alla minimizzazione del rischio di perdita, e a valutazioni di sicurezza, sulla scia della valorizzazione di un sistema di trattamento responsabile (*accountability*) del titolare, che è stato promosso dalla nuova disciplina¹²³. Ma, posta la difficoltà di "tracciare" efficacemente i propri dati in un mondo di *big data*, una tale possibilità dovrebbe essera accuratamente calibrata. Un punto di partenza può essere rappresentato dalla congerie di informazioni che costituiscono dati personali le quali stentano ad essere riassumibili in un unico diritto ma interpretano interessi particolari, oggetto di diversa protezione. La distinzione operata tra dati c.d. sensibili (semi-sensibili o super-sensibili), in ragione della valenza specifica dei diritti fondamentali a questi connessi, e altri dati personali, rispetto ai quali i rischi sui diritti della persona si concentrano in

122 Invero, questo indirizzo si ricollega alle teorie del c.d. paternalismo comportamentale, il cui principale esponente è il giurista Cass Sunstein. Vedi Sunstein, *Effetto nudge: la politica del paternalismo libertario*, trad. it. a cura di Barile, Milano, Egea-Università Bocconi, 2015.

123 Un sistema del genere manterrebbe invariata la risarcibilità (pur non facile) dei danni cagionati per effetto del trattamento.

possibili invasioni della sfera privata non sempre tali da generare un danno alla persona¹²⁴, esprime questa necessità di una classificazione per specifici interessi.

Alla luce di tale distinzione, e considerati i deficit cognitivi riguardanti la prestazione del consenso nella realtà *iper*-connessa, un modello regolatorio potrebbe avere in considerazione la possibilità di un superamento del requisito 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.

Il problema della tutela dei dati personali, in verità, nel regno dell'aggregazione e dei *big data*, è destinato a spostarsi dalla sfera (della protezione) individuale, come dimostrano i *fallimenti* del consenso e delle regole di responsabilità, ad una più ampia collettiva, ovvero a diversi paradigmi delle tutele private, come sembra ipotizzabile nell'ordinamento italiano anche a partire dalla sempre più ampiamente riconosciuta concezione polifunzionale della responsabilità civile, la cui funzione di deterrenza potrebbe essere potenziata nelle violazioni della disciplina dei dati personali. Peraltro, una visione disincantata delle ricadute dei trattamenti sulle libertà personali, in una prospettiva di lungo periodo, imporrebbe di valutare un intervento sul mercato dei dati, sulla loro circolazione e sui trattamenti per finalità commerciali.

124 Da ultimo Reg. 2016/679 cons. 4 «[...] 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 temperato con altri diritti fondamentali in ossequio al principio di proporzionalità». Con riguardo ai dati sensibili, ai sensi del regolamento, scompare l'onere amministrativo di notifica.

Si è acutamente affermato che: «non si può negoziare la modernità se non continuando a continuamente rivelare informazioni a una pluralità di soggetti [...]»¹²⁵. Lo sviluppo della tecnologia ci ha imposto o induce alla “resa” delle informazioni personali, che poi vengono memorizzate ed elaborate per le più disparate finalità: economiche, di condivisione e manifestazione della personalità, di interesse pubblico. Il singolo vedrà – spesso inconsapevolmente – trattati i propri dati personali, senza avere nella maggior parte dei casi contezza di eventuali utilizzi impropri, né decidendo di sottrarsi.

Più efficaci, ai fini di una protezione (come non diffusione incontrollata e immotivata) di dati possono risultare, come detto: la previsione di regole di trattamento, limiti (o divieti)¹²⁶ al trattamento di taluni dati (ad es. quelli a impatto discriminatorio), ovvero più ampie garanzie di anonimizzazione dei dati e da norme tecniche interne di trattamento¹²⁷.

Inoltre, se si intende accogliere la visuale del potenziamento dei diritti ai propri dati, fornendoli di rimedi e in un’ottica di deterrenza, possono essere percorse quelle proposte interpretative che, dando voce anche ad esigenze di una realtà sempre più distante dalla materialità, propongono l’ampliamento dei rimedi esperibili per fattispecie illecite le quali, pur non producendo un danno, sono in grado di generare arricchimenti in capo all’autore dell’illecito¹²⁸. Tuttavia, anche in questo caso, la normale destinazione del dato

125 R. A. POSNER, *ult. op. cit.*, p. 249.

126 «Il divieto resta la forma fondamentale della garanzia della persona» D. MESSINETTI, *op. cit.*, p. 352.

127 La previsione di regole tecniche e quindi di tecnologie conformate (regolamentazione tramite la tecnologia) si rinviene nel GDPR nella previsione della c.d. *privacy by design* (art. 25- in parte già prevista nel codice privacy (articoli 33, 34, 35 e 36) e nel *Disciplinare Tecnico* (Allegato B del Codice Privacy) nonché nella promozione di meccanismi e organismi di certificazione della *privacy* (art. 42). Sul punto, già A. MANTELETO, *Digital privacy: tecnologie “conformate” e regole giuridiche*, in *Privacy digitale. Giuristi e informatici a confronto*, Torino, Giappichelli, 2005, p. 19 ss. Sul fallimento e la reversibilità delle procedure di anonimizzazione, ОНМ, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* 57 UCLA «Law Review» 1701, 2010; nonché, Gruppo di lavoro articolo 29 per la Protezione dei dati, *Parere 05/2014 sulle tecniche di anonimizzazione*, 10 aprile 2014.

128 In materia di c.d. disgorgement, per tutti SIRENA, *La gestione di affari altrui. Ingerenze altruistiche, ingerenze egoistiche e restituzione del profitto*, Giappichelli, Torino, 1999, p. 277.

personale al più ampio novero della raccolta, ovvero dei *big data*, richiederebbe un'attenta valutazione dei criteri di determinazione del *quantum* restituibile o risarcibile¹²⁹.

Ma questa è un'altra narrazione, che tuttavia contribuisce ad arricchire l'insoddisfazione per lo scenario attuale.

129 Nella prospettiva rimediale, suggerisce un diverso sistema di tutele A. MANTELERO, *Personal Data for Decisional Purposes in the Age of Analytics: from an Individual to a Collective Dimension of Data Protection*, 32 *Comp. Law & Secur. Rev.* 2016, p. 238 ss.