IAIC MiBACT DGBIC CREDA

Diritto Mercato Tecnologia

25 Gennaio 2017

Il consenso *al trattamento dei dati personali tra Nuovo Regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione*

Ilaria Amelia Caggiano

Nuova
Editrice
Universitaria

La rivista è stata fondata nel 2009 da Alberto M. Gambino ed è oggi pubblicata dall'Accademia Italiana del Codice di Internet (IAIC) sotto gli auspici del Ministero dei beni e delle attività culturali e del turismo - Direzione generale biblioteche e istituti culturali (DGBIC) e dell'Università Europea di Roma con il Centro di Ricerca di Eccellenza del Diritto d'Autore (CREDA).

Norme di autodisciplina

1. La pubblicazione dei contributi sulla rivista "Diritto Mercato Tecnologia" è subordinata alla presentazione da parte di almeno un membro del Comitato di Direzione o del Comitato Scientifico e al giudizio positivo di almeno un membro del Comitato per la Valutazione Scientifica, scelto per rotazione all'interno del medesimo, tenuto conto dell'area tematica del contributo. I contributi in lingua diversa dall'italiano potranno essere affidati per il referaggio ai componenti del Comitato Scientifico Internazionale. In caso di pareri contrastanti il Comitato di Direzione assume la responsabilità circa la pubblicazione.
2. Il singolo contributo è inviato al valutatore senza notizia dell'identità dell'autore.
3. L'identità del valutatore è coperta da anonimato.
4. Nel caso che il valutatore esprima un giudizio positivo condizionato a revisione o modifica del contributo, il Comitato di Direzione autorizza la pubblicazione solo a seguito dell'adeguamento del saggio.

La Rivista adotta un Codice etico e di buone prassi della pubblicazione scientifica conforme agli standard elaborati dal Committee on Publication Ethics (COPE): Best Practice Guidelines for Journal Editors.

Sede della Redazione

Accademia Italiana del Codice di Internet, Via dei Tre Orologi 14/a, 00197 Roma, tel. 06.8088855, fax 06.8070483, www.iaic.it, info@iaic.it

Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione

Ilaria Amelia Caggiano
Università degli Studi Suor Orsola Benincasa

Abstract: Il contributo analizza criticamente la regola del consenso al trattamento dei dati personali, con particolare riguardo all'attuale realtà tecnologica, quale meccanismo in grado di svolgere una funzione di di autodeterminazione o protezione per l'interessato. Il lavoro si avvale di alcuni risultati dell'analisi comportamentale per la verifica dell'effettività del consenso come mezzo di tutela e di un'analisi giurisprudenziale relativa agli altri rimedi privatistici (risarcimento danni). Alcuni spunti per uno scenario alternativo vengono infine proposti.

The article questions the rule of consent to the proceeding of personal data, especially in the technological context, as a tool of self-determination or protection for the data subject. The work draws on some results from behavioural studies and some Italian judgements regarding other private remedies in data protection law (liability for damages). Some hints for an alternative scenario are finally suggested.

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

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

In questo senso, una delle cifre unificanti del nostro tempo è costituita la centralità dell'informazione e della sua diffusione, in veste ormai essa stessa di bene di consumo e di scambio. L'informazione, nell'era tecnologica, diventa *dato* raccolto massivamente, rapidamente trasmesso, tramite la rete Internet, e avente il più disparato contenuto. In tal modo, l'unità minima dell'informazione, neutrale (*bit*), viene a riguardare non più soltanto la manifestazione del pensiero dell'individuo, ma l'individuo stesso. Esempio ne è l'informazione, inevitabilmente parziale e frammentaria, univocamente a lui riferibile: il dato personale.

Appare chiaro che il flusso continuo di informazioni riguardanti l'individuo, alimentato dalla richiesta individuale di beni e servizi, abbia modificato l'antropologia stessa delle persone, le libertà e i diritti a queste riferibili[1]. Avendo a mente tale variazione può comprendersi (se non condividersi) il sorgere in capo al singolo di un distinto diritto rispetto al dato personale a lui riferibile, configurato in via autonoma rispetto alla sua identità o riservatezza, inizialmente vantato nei confronti delle amministrazioni pubbliche o di pochi soggetti privati, e successivamente di una pluralità di soggetti[2]. Ma lo scenario è ancora in evoluzione[3].

---

[1] 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 "datocentrico" 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 *Dir. info*., 2014, p. 569 ss.

[2] L'idea che il singolo non solo abbia diritto a spazio di vita che non possa essere invaso da terzi (art. 7 Carta dei diritti fondamentali dell'UE), ma che egli abbia il diritto di "governare", o quanto meno tracciare, ogni frammento d'identità che venga detenuto da terzi, interpreta la formalizzazione dell'interesse del singolo alla non esposizione della propria persona all'invasione della propria sfera da parte dei terzi.

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*[4]), è in grado di aggregare un tale ammontare di dati, da consentire che questi ultimi, una volta analizzati, si prestino a fornire il quadro del singolo, della società globale, o ogni caso di grandi comunità, da molteplici punti di vista. Fanno così ingresso nella società dell'informazione i *big data*: *dataset* che per la loro estensione in volume, velocità e varietà consentono di estrarre informazioni aggiuntive, tali da determinare modelli di *business* e mercati o utilizzi scientifici di questo sapere digitale[5]. I dati personali, che entrano nella disponibilità di una molteplicità di soggetti pubblici e privati, vengono più significativamente elaborati da coloro che hanno i più estesi *database* e che si vengono a trovare in posizioni quasi monopolistiche o, in ogni caso, dominanti. Tale disponibilità dei dati segna, altresì, il passaggio a una sempre più pervasiva profilazione dei singoli, risalendo tramite la cronologia delle loro attività, alle loro preferenze, interazioni, stili di vita, al fine di proporre prodotti o pubblicità mirata (finalità commerciali); al monitoraggio predittivo di più ampi gruppi sociali[6]; alla capacità di correlare fenomeni del più disparato genere con alta probabilità[7].

---

[3] 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.

[4] Sull'IoT, preliminarmente, P. Paganini, *Verso l'internet delle Cose,* in *Dir. ind.*, 2015, p. 107 ss..

[5] 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: R. Moro Visconti, *Valutazione dei* big data *e impatto su innovazione e* digital branding, in *Dir. Industriale,* 2016, p. 46 ss.

[6] Si può far riferimento ai motori di ricerca, a *social network,* ai più comuni *marketplaces* (Google, Facebook, Amazon).

[7] Com'è stato nel caso della mappatura dell'influenza da parte di Google in tempo reale e 2 settimane prima delle istituzioni governative. Sul punto, M. Bogni, A. Defant, Big data: *di-*

Da un punto di vista fenomenico, la raccolta dei dati personali si realizza in vario modo: in occasione 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 condivisione); da parte di motori di ricerca[8].

La circolazione dei dati, attraverso la vendita a terze parti (anche per finalità pubblicitarie), è fonte di profitto per il titolare del trattamento [9]. Lo sfruttamento commerciale delle informazioni personali come beni immateriali disponibili e negoziabili rappresenta la principale attività delle imprese che forniscono servizi digitali e una realtà fortemente caratterizzante l'odierno quadro economico[10]. Appare, pertanto, evidente come i dati per-

---

ritti IP e problemi della privacy, in *Dir. Industriale,* 2015, p. 117 ss.

[8] A.R. Pipoli, *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, ovverosia 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*».

[9] «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». A.R. Pipoli, *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».

[10] Si pensi solo al fatto che Google, diventata la seconda società al mondo per valore in Bor-

sonali, e il loro trattamento, siano terreno non solo di libertà e diritti fondamentali, ma – in virtù del loro valore economico – di contenuto patrimoniale, come una qualificazione giuridica delle "transazioni" che li hanno ad oggetto dovrebbe far emergere[11].

2. L'ambito dell'indagine

Il sintetico scenario appena descritto può costituire lo sfondo per riflettere sulle ragioni e l'efficacia dell'attuale regolamentazione in senso protettivo del diritto alla protezione dei propri dati, con particolare riguardo ai trattamenti svolti da soggetti privati e alla luce della recente entrata in vigore del più incisivo provvedimento europeo in materia degli ultimi venti anni, il quale esplicitamente guarda alla realtà digitale[12].

Il livello di analisi, cui s'intende far riferimento, è duplice:

1. da un lato sembra opportuno verificare se gli strumenti di regolazione previsti siano, in prospettiva, funzionali agli obiettivi di tutela e quali più precisamente siano questi ultimi[13]. Ci si concentrerà, in particolare, sul con-

---

sa — con 522 miliardi di dollari di capitalizzazione, poco sotto i 587 miliardi di Apple, con un fatturato in crescita anche nel primo trimestre 2016. (fonte: 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)

[11] 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 suscettibile di una valutazione economica e, quindi, di tipo patrimoniale, che – a nostro modo di vedere - viene a caratterizzare la complessiva operazione economica. La qualificazione delle operazioni negoziali in cui si inserisce una prestazione di consenso, oltre a porre in risalto la requisito della onerosità/gratuità (in tema 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, 2005. Sulla qualificazione dell'atto di prestazione del consenso (nel senso di atto di consenso dell'avente diritto, atto giuridico in senso stretto, atto negoziale unilaterale), *ex multis*, S. Mazzamuto *Il principio del consenso e il potere della revoca* in Aa. Vv., *Libera circolazione e protezione dei dati personali*, a cura di R. Panetta, t. I, Milano, Giuffrè, 2006, p. 994 ss.

[12] Regolamento (UE) 2016/679 in GUUE L119 del 4 maggio 2016, la cui disciplina si applicherà a decorrere dal 25 maggio 2018 (art. 99, par. 2).

[13] Questa prima fase prevede, in particolare, l'analisi di alcuni risultati che attingono alle

senso come base giuridica legittimante il trattamento dei dati personali, al fine di verificare l'utilità della sua previsione (ciò che si dirà *l'efficacia normativa* o *effettività della tutela*);

2. tenuto conto del risultato del primo livello dell'analisi, si passerà ad esaminare il contenuto del diritto alla protezione dei dati realisticamente tutelabili, e meritevoli di tutela nell'ottica della protezione della identità, dello spazio di vita e della non discriminazione della persona, conformemente ai principi generali (qui valori, in quanto libertà personali) dell'ordinamento nazionale ed europeo.

Ciò può portare a configurare non solo una diversa graduazione della tutela dei dati rispetto alla loro incidenza sui diritti fondamentali dell'individuo, ma meccanismi di tutela diversi da quelli attuali[14].

3. Il "consenso" come presupposto per il trattamento dei dati personali e il Reg. (UE) 2016/679

Nel quadro della complessiva disciplina del trattamento dei dati personali, che prevede articolati obblighi e strutture di controllo, destinate a moltiplicarsi con l'adozione del nuovo Reg. (UE) 2016/679[15], il consenso

---

scienze psico-comportamentali con particolare riguardo all'attitudine degli individui rispetto alla manifestazione del consenso al trattamento di dati personali. In generale sugli studi comportamentali nella dottrina giuridica, tra gli altri L. Arnaudo, *Diritto cognitivo. Prolegomeni a una ricerca*, in *Politica dir.*, 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 *Aust. Law Jour.* 2014, p. 19 ss.

[14] In sintesi, v'è da chiedersi: quali siano, al di fuori della (vuota?) 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.

[15] In aggiunta ad una procedura di trattamento dei dati già sufficientemente strutturata e regolata (quella prevista dalla normativa interna), e che appare sostanzialmente confermata nel nuovo assetto, le più recenti novità portate dal Reg. 2016/679 possono sintetizzarsi nei punti che seguono: 1. Introduzione del diritto alla portabilità dei dati da un titolare del trattamento ad un altro (come nel caso di passaggio di provider e salvataggio dei messaggi di posta elettronica e dei contatti) – art. 20; 2. Procedure e adeguatezza per il trasferimento dei dati extra-Ue; 3.- Inasprimento delle sanzioni amministrative pecuniarie in caso di *data breach* e violazioni del regolamento (art. 83) e obbligo di comunicare all'Autorità nazionale le eventuali

dell'interessato continua a mantenere un ruolo centrale quale presupposto del trattamento dei dati personali.

Il Regolamento 2016/679, infatti, 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 imprenditoriali e agli adempimenti in capo ai responsabili e titolari, spostando in capo a questi ultimi il rischio delle attività, ma non significativamente con riguardo al fondamento giuridico che legittima il trattamento[16].

I titolari sono tenuti ad adottare una serie di misure aventi carattere tendenzialmente preventivo che caricano la finalità di protezione sull'organizzazione aziendale e su strumenti a loro volta tecnologici. 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)[17]; la nomina obbligatoria, in taluni casi[18], 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

---

violazioni di dati personali (cons. 85); 4. Principio di responsabilizzazione (*accountability* – art. 2) tramite introduzione di nuove procedure, figure di garanzie come la valutazione d'impatto (cons. 84 ss. e art. 35 ss.), in caso di trattamenti con rischi elevati e della privacy by design; 5. Figure di controllo Data Protection Officer – *Responsabile della protezione dei dati* (art. 37 ss., cons. 97), incaricato di assicurare una gestione corretta in imprese ed enti; 6. Promozione di condici di condotta e meccanismi di certificazione rilasciati da un soggetto abilitato o dall'autorità di protezione dati (art. 35 ss.); istitutzione del Comitato Europeo per la protezione dei dati

[16] A. Ciccia Messina, 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.

[17] Ma già in art. 17 cod. privacy.

[18] La figuda 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.

enti e fungere da punto di contatto autorità.

A tali misure si accompagna: 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 Europea[19], 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-UE[20].

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.

In tale contesto, il consenso è uno dei "fondamenti legittimi" (secondo la terminologia della Carta di Nizza, o base giuridica) per avviare il trattamento dei dati personali[21], sia con riguardo ai dati personali in generale

[19] 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

[20] È 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.

[21] 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

(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)[22].

Ora definito come «espressione di manifestazione dei 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)[23], 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 accettazione[24]. In proposito, si deve aver in mente non solo l'utilizzo di strumenti digitali ma, inevitabilmente, la già dilagante diffusio-

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 considerate 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.

[22] Nel mantenimento del meccanismo informativa + consenso, si conferma la necessità di un consenso preventivo e 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 Aa. Vv., *Privacy digitale. Giuristi e informatici a confronto*, Torino, Giappichelli, 2005, 81 ss.

[23] Recita il vigente art. 23 cod. privacy: «Il consenso è validamento 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»

[24] 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 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».

ne 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 (espresso), 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 italiano[25]), tale dovendo essere qualsiasi consenso, sia per il legislatore europeo (cons. 32), sia per il legislatore italiano (art. 23 cod. privacy)[26]. 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'interessato[27]. L'informazione resta comunque dovuta, anche quando non sia propedeutica ad una successiva manifestazione di volontà[28].

---

[25] F. Galgano, *Il contratto*, II ed., Padova, 2011, p. 126.

[26] 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 ss.

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

[28] 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,

4. Critica alla rilevanza del consenso e del processo di *decision-making* per le finalità di protezione dei dati personali.

La disciplina appena descritta pone, quindi, la determinazione dell'individuo rispetto al trattamento da parte di terzi delle informazioni personali a lui riferibili in una posizione rilevante nella complessiva attività di trattamento, in certa coerenza con la configurazione del diritto alla protezione dei dati quale libertà fondamentale nello spazio giuridico europeo (art. 8 Carta di Nizza) [29].

Tale strategia ci appare, tuttavia, non pienamente performante le ragioni della tutela dei soggetti destinatari, rappresentate dalla protezione del dato personale e dalla gestione dello stesso da parte dell'interessato[30].

Il problema della "vuota cerimonia" [31], che si celebra alla sottoscrizione di qualsiasi formulario predisposto, si ripropone in maniera accentuata con riguardo al consenso informato in materia di *privacy*, ove la tutela del dato personale è percepita dall'interessato come estranea all'operazione economica che egli sta compiendo. Se è vero che l'informativa in questo caso può assumere un ruolo non tanto di colmare asimmetrie informative, quanto di avviare il controllo dell'interessato sul procedimento in cui si concreta l'attività di trattamento [32], resta fondato il dubbio che come per l'asimmetria, così anche per il controllo, l'informazione prestata non sia in grado di influire sulla consapevolezza dell'atto di volontà del singolo[33].

In proposito, una vasta letteratura di studi comportamentali dimostra

---

sebbene non espressamente prescritta come trasparente, già art. 13 cod. privacy.

[29] È da segnalare, tuttavia, come uguale centralità alla disciplina del consenso sia prevista in ordinamenti imperniati ad una visione "proprietaria" dei dati personali.

[30] 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 informativa.

[31] S. Patti, *Consenso*, sub *art. 23)*, in Aa. Vv. *La protezione dei dati personali. Commentario* a cura di C.M. Bianca, F. D. Busnelli, t. I, Padova, Cedam, 2007, p. 541 ss.

[32] Mazzamuto Il principio del consenso e il potere della revoca cit. spec. 1004.

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

come le decisioni assunte in materia di *privacy* si sottraggano completamente al paradigma della scelta razionale e che in ogni caso, nel momento in cui gli interessati prestano il consenso, siano disposti a scambiare i propri dati anche per un minimo vantaggio o ricompensa[34]. Ciò anche nell'ipotesi in cui abbiano precedentemente affermato di desiderare un alto grado di tutela della propria *privacy*. Le evidenze empiriche dimostrano allora come, in aggiuta 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 si distaccano totalmente da un mondo, quello dell'informativa e del consenso consapevole, che presuppone comportamenti ispirati a razionalità[35].

È dubbio allora che il consenso possa rappresentare un meccanismo avente una qualche funzione per la protezione del diritto del singolo ai suoi dati personali. Tali considerazioni reclamano una certa attenzione da parte dell'interprete e del legislatore (!), il quale dovrebbe, infine, prenderne atto.

Come anticipato, il consenso dell'interessato, ove richiesto, rappresenta soltanto il fondamento di un ben più articolato procedimento che ha la chiara funzione di rendere controllabile il trattamento dei dati effettuato dal titolare.

---

[34] L.J. Strahilevitz, Toward a Positive Theory of Privacy Law, in Harv. Law Rev., 1999, p. 1; D.J. Solove, Privacy self-management and the Consent Dilemma, in Harv. Law Rev., 2013, 1880; F.Z. Borgesius, Informed consent: We Can Do Better to Defend Privacy, in IEE, 2015, p. 103 - 107; Id. Behavioural Sciences and the Regulation of Privacy on the Internet, in Amsterd. Law School Research Paper, 2014, p. 54; A. Acquisti, Privacy, in Riv. pol. Econ., 2005, p. 319; S. Barocas, 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; O. BenShahar, A. Chilton, Simplification of Privacy Disclousure: An Experimental Test, in Journ. Legal Studies 2015, p. 45.

[35] 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. In punto, S. Patti, *Consenso*, cit.. 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. Senza giungere ad accogliere prospettive così eccentriche, che porrebbero peraltro un grave problema di coordinamento con il sistema degli atti giuridici, l'analisi fornita ci sembra dimostri, invece, l'inefficacia della normativa rispetto alla *ratio* di tutela.

Si potrebbe supporre, allora, che il consenso, quale suggello dell'informativa, possa svolgere, quanto meno, la funzione di richiamare l'attenzione del titolare e responsabile del trattamento al controllo di regolarità dello stesso. Anche rispetto a tale finalità, non si vede come l'informazione fornita a terzi possa compulsare a comportamenti già previsti, e sanzionati specificamente, da distinti obblighi di legge.

Quale dato fornito dell'esperienza 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 (caso Google)[36]. Tuttavia, appare dubbia l'aspettativa che il "miglioramento" dell'informativa sia realmente in grado di incidere sulla consapevolezza dell'utente, come dimostrano recenti studi aventi ad oggetto proprio l'informativa Google.[37]

Ci sembra evidente che se si resta nella logica della informativa o dei suoi progressivi, minimali miglioramenti, il rischio è di rimanere all'interno

[36] Google, che 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 al link http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3740038
L'numero di provvedimenti dell'Autorità in materia di informativa (artt. 13 e 161 cod. privacy) sono 642 (fonte: sito GarantePrivacy)

[37] Sul punto, O. BenShahar, 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?*, in *Journ. Legal Studies*, 2017, p. S69 - S95 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 trattemnto altamente intrusivo, non siano cambiate in ragione del linguaggio dell'informativa, ma delle norme sociali e dell'esperienza tecnologica. Si segnala come analoghi studi, che si avvalgono in particolare di strumenti di misurazione di analisi comportamentale, siano attualmente in corso in Italia. Sul punto ci sia consentito rinviare 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 Aa. Vv., *Nodi virtuali, legami informali, Internet alla ricerca delle regole,* a cura di D. Poletti e P. Passagna, in corso di pubblicazione, p. 53 ss.

di un labirinto che non porta a risultati significativi[38].

Peraltro, la prestazione *ex ante* del consenso 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 dei dati, anche per la complessità di governo del mercato degli stessi.

Prova ne è che lo stato attuale della sorveglianza e della tecnologia non consente in ogni caso di evitare c.d. 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[39], e può spiegarsi in virtù della massiva richiesta diffusione dei dati e della loro elaborazione attraverso algoritmi.

Ritorna allora, per questa via, il riferimento alla realtà complessa della circolazione dei dati, al mondo dei *big data*, alle loro regole tecniche di funzionamento, difficilmente controllabili dal consenso del singolo e probabilmente neppure pienamente intercettabili dal requisito della determinatezza delle finalità di trattamento[40].

Il quadro che deriva dalla normativa in materia di consenso e di obblighi dei soggetti coinvolti nel trattamento è una macchina complessa che comporterà, in progresso di tempo e alla luce della nuova normativa, costi di *compliance* per le imprese, rispetto ai quali andrà verificato l'effettivo incremento nella tutela dei diritti dei singoli.

5. Alcune proposte per uno scenario complesso.

Per quanto sommariamente esposto, a nostro modo di vedere, la tutela dei dati personali non riceve pertanto beneficio dall'opzione richiesta al

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

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

[40] Art. 5, §1, lett. *b)* GDPR e art. 11, co. 1, lett. *b)*, Codice Privacy.

singolo e può risultare opportuno ripensare i limiti del consenso e del trattamento, sviluppando alcune riflessioni critiche.

Già la Carta dei diritti fondamentali UE[41] individua il consenso quale uno soltanto dei possibili legittimi fondamenti previsti dalla legge al trattamento dei dati di carattere personale lasciando spazio anche a diversi presupposti del trattamento. A ben vedere e fuor di retorica, la prestazione del consenso non è regola assoluta, né centrale, nel nostro ordinamento, come confermato anche dalla normativa che troverà applicazione a partire dal 2018, la quale, pur criticabilmente prescrivendo la necessità di un consenso espresso manifestato *ex ante,* ne opera poi una esplicita restrizione, considerando espressamente la finalità di *marketing* diretto come legittimo interesse del titolare del trattamento (cons. 47), tale da escludere, appunto, il previo consenso dell'interessato[42].

In questo quadro, allora potrebbe esservi ulteriore spazio per un sistema in cui la prestazione del consenso venga interpretata restrittivamente, o non venga più richiesta (in una prospettiva *de iure condendo*), restando all'interessato il diritto al controllo sui propri dati, ove intercettati, e ad un trattamento conforme a 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 disciplina[43]. Va poi precisato che il fatto che il trattamento possa esser basato su fondamenti legittimi diversi dal consenso non esclude, almeno in via di principio, il necessario bilanciamento di questi con le libertà fondamentali, ma allo stesso tempo consente di prescindere dall'"illusione del consenso" quale strumento di

[41] Tale configurazione alternativa è presente anche nella normativa interna, agli artt. 24, 43, 44 del d.lgs. 30 giugno 2003, n. 196, c.d. Codice Privacy

[42] 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 restringe la fattispecie non all'attività di chi tratta i dati personali (tipologia del trattamento, nel quale può rientrare l'invio di materiale pubblicitario) ma l'attività cui i dati personali medesimi si riferiscono (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)

[43] Un sistema del genere manterrebbe invariata la risarcibilità dei danni cagionati per effetto del trattamento.

controllo sui propri dati. Un tale approccio consentirebbe, invece, di superare una logica che induce pericolosamente a ritenere l'interessato in grado di controllare e proteggere autonomamente i propri dati, ovvero gli conferisce poteri non effettivamente esercitabili o diritti che, se violati, restano comunque privi di sanzione.

Più efficaci, ai fini di una protezione (come non diffusione incontrollata o non adeguatamente giustificabile) di dati, si ritiene possano risultare: la previsione di regole di trattamento, limiti (o divieti) a monte per alcune tipologie di trattamento e/o per taluni dati, ovvero più ampie garanzie di anonimizzazione dei dati e da norme tecniche interne di trattamento[44].

In questa prospettiva, appare opportuno distinguere all'interno delle tipologie di dati, già presenti nella normativa europea e italiana. Nel sistema italiano la distinzione assume la nomenclatura di dati c.d. sensibili e personali, genericamente intesi. Per i primi, che secondo la terminologia attualmente utilizzata nella prassi si possono caratterizzare come semi-sensibili o super-sensibili, è previsto un più incisivo controllo amministrativo 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 possibili invasioni della sfera privata[45], non sempre tali da generare un danno, e che non necessitano di un sistema di previa notifica e relativo controllo. Questa distinzione, presente nel più recente regolamento europeo che

[44] 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. Mantelero, Digital privacy: *tecnologie "conformate" e regole giuridiche*, in Aa. Vv., *Privacy digitale. Giuristi e informatici a confronto*, Torino, Giappichelli, 2005, p. 19 ss. Sul fallimento e la reversibilità delle procedure di anonimizzazione, P. Ohm, *Broken Promises of Privacy: Responding to the Surprisisng Failure of Aninymization*, in *UCLA Law Rev.*, 2010, p. 1701; Gruppo di lavoro articolo 29 per la Protezione dei dati, Parere 05/2014 sulle tecniche di anonimizzazione, 10 aprile 2014.

[45] 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 contemperato 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.

tuttavia elimina la burocrazia delle autorizzazioni preventive, potrebbe aprire ad un trattamento differenziato, tra dati personali e dati sensibili (nelle diverse graduazioni al suo interno), ma in un senso rinnovato. In una prospettiva *de iure condendo*, il consenso potrebbe essere mantenuto per limitate classi di dati sensibili, per le quali è prospettabile l'astratta eventualità di un attenzione effettiva da parte dell'interessato nel momento in cui viene richiesto , e – laddove si assumesse la protezione dei dati in senso specifico e incisivo – l'unica alternativa allo scenario esistente potrebbe essere costituito da limiti a trattamenti che comportino pregiudizio anche come risultato dell'elaborazione e combinazione di più dati personali/sensibili. Tale prospettiva, però, dovrebbe presupporre una seria posizione da parte del legislatore europeo con riguardo allo sviluppo dei mercati dei dati e all'impatto di lungo periodo sui diritti della persona, regolando la diffusione di informazioni[46].

Il problema centrale, quindi, è rappresentato dalle regole e limiti al trattamento e prescinde dalla scarsamente efficace previsione di meccanismi di selezione *ex ante* da parte dell'interessato (*consenso*).

Ma la protezione dei dati personali, dal punto di vista privatistico, si trova ad essere limitata anche nella fase rimediale. 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. A meno di sottrarsi alle logiche di funzionamento della società attuale, il singolo vedrà – spesso inconsapevolmente – trattati i propri dati personali, senza avere nella maggior parte dei casi contezza di eventuali utilizzi impropri.

Tuttavia, anche l'eventuale conoscenza del trattamento illecito dei propri dati personali può non comportare la disponibilità di un rimedio privatistico in capo alla persona fisica, per l'assenza di un danno[47] – ovvero per il

[46] R. A. Posner, *ult. op. cit*., p. 249: «non si può negoziare la modernità se non continuando a continuamente rivelare informazioni a una pluralità di soggetti […]»

[47] Il danno patrimoniale da illecito trattamento dei dati personali trova ingresso nell'ipotesi di illegittimo trattamento di credenziali bancarie/finanziarie, come nell'ipotesi di *pishing* (da ult. Cass. civ., sez. I, 23.05.2016, n. 10638, in *DeJure*). Diversa è l'ipotesi delle informazioni

carattere bagattellare dello stesso (si pensi allo *spamming*)[48], o ancora per la difficoltà di rintracciare il titolare o responsabile del trattamento che abbia dato origine o partecipato alla produzione dell'evento dannoso (potrebbe darsi il caso di una profilazione non autorizzata che conduca ad una diffusione di gusti personali del singolo che egli intende mantenere riservati).

Il problema che si pone è quello relativo alle ipotesi concrete di configurabilità di un danno serio in capo all'interessato in caso di violazione della normativa sulla protezione dei dati, nonché, più specificamente, di risarcibilità del diritto alla protezione dei dati, indipendentemente dalla lesione altri diritti fondamentali. La latitudine della questione è ampia e non può essere percorsa in questa sede, ma consente di completare il quadro problematico dell'efficacia degli strumenti privatistici a tutela della protezione dei dati personali[49].

---

sulle relazioni creditizie, si pensi al caso della comunicazione di dati finanziari del singolo da parte di istituti bancari a centrali rischi, che portino alla mancata stipulazione di altro contratto finanziario da parte del cliente segnalato. In tali ipotesi, se il rimedio *lato sensu* amministrativo (provvedimento del Garante, oggi) impedisce all'impresa commerciale di trattare dati raccolti, per determinate finalità dai Sistemi di informazione creditizia, più dubbia sarebbe la configurabilità del danno per la mancata stipula del contratto, ove andrebbe dimostrata specificamente tanto l'illegittimità della segnalazione (che risulta allo stato ammessa anche per la morosità di una singola rata) quanto la causalità diretta rispetto alla mancata stipula di altro 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]. Sul punto, il GDPR interviene prevedendo che le decisioni che producono effetti giuridici (concessioni di prestiti etc.) non possono essere basate su trattamento automatizzato di dati (profilazione) (cons 71).

[48] In proposito, da ultimo, Cass., 11 gennaio 2016, n. 222, in *DeJure* con nota di M. Alovisio, in *Risarcimento del danno per diffusione indebita di dati sanitari,* in *Dir. Giust.*, 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.

[49] Per una più dettagliata analisi, ci sia consentito reinviare al nostro *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale* in corso di pubblicazione per i tipi della Giappichelli

Anche nei casi in cui risulta configurabile un danno non patrimoniale per violazione dei dati personali[50], si pongono inevitabili problematiche connesse alla liquidazione del danno, come evidenziato in recenti casi[51].

La carenza rimediale per il privato in caso violazioni dei dati personali *tout cour*, che è correlata al carattere non rivale per quanto escludibile del dato stesso[52], tende a confermare che l'affermazione del diritto alla protezione dei dati non sia efficacemente tutelabile per il privato, al di là dell'efficacia dei controlli amministrativi e giurisdizionali sulle regole del trattamento.

Si confermerebbe allora che la reale finalità di tutela del diritto a veder protetti i propri dati (specialmente non sensibili) può riguardare la tutela dei mercati o la protezione di una più generale condizione dell'esistenza umana, ma tende – allo stato – a sfuggire alla sfera del singolo, in via preventiva (consenso) o successiva (risarcimento danni) .

Sul secondo aspetto, se si intendesse accogliere la visuale del potenziamento dei rimedi sui diritti ai propri dati, in un'ottica di deterrenza, andrebbero allora 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'illecito[53]. Tuttavia, anche in questo caso, la normale destinazione del dato personale al più ampio novero della raccolta, ovvero dei *big data*, richiederebbe un'attenta valutazione dei criteri di determinazione del *quantum* restituibile o risarcibile[54].

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

---

[50] Una ricerca giurisprudenziale condotta sulla banca dati *DeJure,* produce un risultato di 115 provvedimenti in materia di violazioni dell'art. 15 del Codice Privacy.

[51] 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.

[52] V. Visco Comandini, Il ruolo della privacy nella competizione per l'accesso delle risorse pubblicitarie su Internet, in Dir. Econ. e Tecn. Della Privacy, 2012, n. 1, p. 1 ss.

[53] In materia di c.d. disgorgement, per tutti P. Sirena, La gestione di affari altrui. Ingerenze altruistiche, ingerenze egoistiche e restituzione del profitto, Torino, Giappichelli, 1999, p. 277.

[54] 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 Collectivce Dimension of Data Protection, in Comp. Law & Secur. Rev., 2016, p. 238 ss.

Diritto Mercato Tecnologia

Numeri Speciali

2016 Lo Statuto Etico Giuridico dei Campioni Biologici Umani
a cura di Dario Farace

La rivista "Diritto Mercato Tecnologia" intende fornire un costante supporto di aggiornamento agli studiosi e agli operatori professionali nel nuovo scenario socio-economico originato dall'interrelazione tra diritto, mercato e tecnologia, in prospettiva interdisciplinare e comparatistica. A tal fine approfondisce, attraverso studi nei settori privatistici e comparatistici, tematiche afferenti in particolare alla proprietà intellettuale, al diritto antitrust e della concorrenza, alle pratiche commerciali e alla tutela dei consumatori, al biodiritto e alle biotecnologie, al diritto delle comunicazioni elettroniche, ai diritti della persona e alle responsabilità in rete.