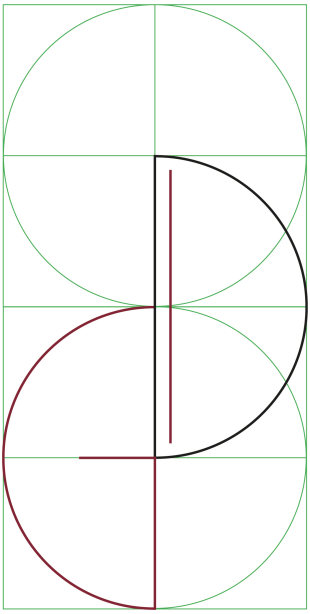
Materiali e documenti

Annuario 2021 Osservatorio Giuridico sulla Innovazione Digitale

Yearbook 2021 Juridical Observatory on Digital Innovation

a cura di
Salvatore Orlando e Giuseppina Capaldo



University Press

SAPIENZA UNIVERSITÀ EDITRICE

Collana Materiali e documenti 75

Annuario 2021
Osservatorio Giuridico sulla Innovazione Digitale

Yearbook 2021
Juridical Observatory on Digital Innovation

a cura di Salvatore Orlando e Giuseppina Capaldo

SAPIENZA
UNIVERSITÀ EDITRICE
2021

Sapienza Università Editrice
Piazzale Aldo Moro 5 – 00185 Roma

www.editricesapienza.it
editrice.sapienza@uniroma1.it

Iscrizione Registro Operatori Comunicazione n. 11420

ISBN 978-88-9377-186-3

DOI 10.13133/9788893771863

Pubblicato nel mese di luglio 2021

Impaginazione/layout a cura di: Enzo Maria Incutti

In copertina: Michela Tenace, *Studio per il logo OGID/JODI* (2021), archivio dell'A.

Indice

Prefazione

L'idea e la realizzazione del presente *Annuario* sono maturate nell'ambito delle attività seminariali, di confronto e di studio promosse nel corso del 2020 dall'Osservatorio Giuridico sull'Innovazione Digitale (OGID), costituito presso il Dipartimento di Diritto ed Economia delle Attività Produttive dell'Università Sapienza di Roma (https://web.uniroma1.it/deap/ogid).

L'Osservatorio promuove lo studio delle relazioni tra le tecnologie digitali e il diritto privato, attraverso una serie di attività, tra le quali la tenuta di *webinar* con cadenza settimanale, la cura di pubblicazioni e la partecipazione alle procedure di consultazione pubblica delle istituzioni della Unione europea sulle proposte normative aventi ad oggetto le tematiche dell'innovazione digitale.

Nel corso del 2020 OGID ha organizzato 27 *webinar*, e circa 30 nel 2021. I relatori provengono da numerose Università italiane e straniere. Alcuni *webinar* sono tenuti in lingua inglese, e anche i relatori non accademici sono italiani e stranieri.

OGID cura dal 2020 la rubrica di aggiornamento "*Diritto e nuove tecnologie*" della rivista trimestrale *Persona e Mercato* (rivista di fascia A)[1].

---

[1] Numeri del 2020: 1/2020 – http://www.personaemercato.it/wp-content/uploads/2020/03/Osservatorio-1-2020.pdf; 2/2020 – http://www.personaemercato.it/wp-content/uploads/2020/05/Osservatorio.pdf; 3/2020 – http://www.personaemercato.it/wp-content/uploads/2020/09/Osservatorio-14.9.2020.pdf; 4/2020 – http://www.personaemercato.it/wp-content/uploads/2020/11/Osservatorio.pdf
Numeri del 2021: 1/2021 – http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio.pdf; 2/2021 - http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio-1.pdf

I contributi pubblicati in questo *Annuario* hanno ad oggetto temi trattati dagli Autori nei *webinar* dell'Osservatorio (nei quali hanno preso parte come relatori) o nella Rubrica "Diritto e nuove tecnologie" sulla rivista *Persona e Mercato*.

Sono contributi che coprono una varietà di temi di diritto privato legati all'innovazione digitale.

Li presentiamo seguendo l'ordine alfabetico degli Autori.

Buona lettura!

I Curatori

Salvatore Orlando Giuseppina Capaldo

6. Regolare l'irregolabile: il consenso al trattamento dei dati nel GDPR

Andrea Maria Garofalo

6.1. Introduzione

Di fronte alla disciplina del consenso al trattamento, che come ben noto costituisce una delle basi giuridiche ammesse dal GDPR per il trattamento dei dati personali, la sensazione che mi pare emerga è – usando un eufemismo – di insoddisfazione.

Tutto il GDPR, infatti, è percorso da una considerazione di fondo: gli individui, i singoli, le persone fisiche non sono idonee a tutelare i loro interessi in materia di protezione dei dati. Lo dimostra l'attenzione verso i controlli interni ed esterni dell'attività di trattamento[1]; lo attesta il principio di responsabilizzazione, che investe il titolare del trattamento dell'onere di valutare e gestire il rischio dello stesso trattamento[2].

Se questo è vero, suona a me quanto meno strano – sempre in senso eufemistico – che questi stessi individui, prima reputati inidonei a tutelarsi, siano abilitati a disporre dei loro stessi dati, addirittura creando una base per il loro trattamento e così rendendo quest'ultimo lecito.

Se lo si ammette, si apre uno scenario di ricerca assai interessante: v'è prima da chiedersi perché, apparentemente in modo contraddittorio, le discipline di protezione dei dati che si sono susseguite nel tempo abbiano ammesso il consenso e quali problemi emergano da questo riconoscimento legislativo[3]; v'è poi da domandarsi come il consenso

---

1 Artt. 24 ss.

2 Art. 24.

3 V. § 2.

sia attualmente regolato (a livello legislativo e interpretativo)[4]; ancora, v'è da verificare se anche l'attuale disciplina di questo atto di volontà presenti delle criticità[5]; infine, deve indagarsi se la ricostruzione dogmatica dell'atto di consenso o una revisione interpretativa o legislativa della sua disciplina consenta di ripianare – almeno in parte – quelle storture cui la stessa esistenza di una simile base legale dà vita e che ancora oggi risultino non superate[6].

A quest'indagine, da svolgere per lo più sul piano eurounitario, sono dedicate le pagine che seguono.

6.2. Funzioni e disfunzioni, da un punto di vista generale, del consenso

Come noto, il trattamento dei dati personali, allorché si rientri entro l'ambito di applicazione del GDPR (in linea di massima: trattamento automatizzato), può avvenire solo se è presente una "base" che lo rende lecito (art. 5, par. 1, GDPR). Tra le basi per il trattamento, accanto all'esecuzione di un contratto, all'adempimento di un obbligo legale o all'esecuzione di un compito in senso lato pubblico, alla salvaguardia di interessi vitali di una persona e al legittimo interesse, troviamo il consenso dell'interessato dal trattamento (art. 6, par. 1, GDPR). E anche con riferimento ai dati "sensibili" (o, meglio, ai dati rientranti in "categorie particolari") possiamo trovare, accanto a un divieto generale di trattamento e alla sua disapplicazione allorché sussistano talune specifiche basi (tra cui manca però l'esecuzione di un contratto e il legittimo interesse), il consenso dell'interessato quale condizione di liceità del corrispondente trattamento (art. 9, par. 2, GDPR).

Emerge con nitidezza, già da questi brevi cenni, la particolarità del consenso: mentre in ogni altro caso il bilanciamento tra gli interessi del titolare del trattamento e i rischi per le libertà, i diritti e gli interessi del *data subject* è stato già compiuto dal legislatore europeo (fermo restando che esso può e deve, in forme e modi di volta in volta diversi,

4 V. § 3.

5 V. § 4.

6 V. §§ 5 e 6.

venire specificato in concreto), nell'ipotesi del consenso il bilanciamento è posto in essere, a suo piacimento, dall'interessato[7]. In tal modo, dunque, viene inserita nel GDPR una condizione di liceità del trattamento che, anziché essere *content-based*, risulta *consent-based* e che, per l'effetto, permette di superare i margini del sistema del Regolamento ogni qual volta essi appaiano in concreto eccessivamente ristretti[8].

Se questa è, banalmente, la ragione fondante del consenso, altrettanto semplice è accorgersi delle disfunzioni che il consenso stesso reca in sé e, una volta ammesso, introduce nell'ordinamento.

Studi recenti hanno, infatti, confermato quanto è sotto gli occhi di tutti noi: la materia della protezione dei dati è dominata da un fortissimo disallineamento tra la realtà delle cose e l'esperienza che ogni utente ne fa giornalmente.

Senza scendere nei dettagli, basterà rilevare che, solitamente, le informative in materia di trattamento dei dati personali, così come le richieste di consenso, sono troppo lunghe per immaginare che il titolare dei dati le legga e le analizzi prima di scegliere se dare il suo consenso. Anche se poi ciò avvenisse, l'interessato difficilmente le capirebbe: o, meglio, comprenderebbe i rischi che il trattamento porta con sé. Difatti, gli utenti di regola sottovalutano i rischi che l'utilizzo dei loro dati comporta (rischi legati non solo e non tanto alla compressione della

---

[7] Si consenta, su questi temi, il rinvio a A.M. GAROFALO, *Protection and Free Movement of Personal Data in EU Law*, in M. SCHMIDT-KESSEL, *European Economic Constitution. German-Italian Dialogue for a Solidarity-oriented Common Market*, Jena, 2020, in corso di pubblicazione.

[8] Del resto, se è vero che il consenso non è la regola rispetto ad altre eccezioni (ossia, rispetto alle altre basi), è vero anche che esso formalmente non è altro che "una condizione tra le altre possibili" (in tal senso v. F. CAGGIA, *Il consenso al trattamento dei dati personali nel diritto europeo*, in *Riv. dir. comm.*, 2019, I, p. 406; F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in AA. VV., *Il nuovo Regolamento europeo sulla* privacy *e sulla protezione dei dati personali*, diretto da G. Finocchiaro, Bologna, 2017, p. 138 ss.). Da un punto di vista sostanziale, tuttavia, il consenso è una condizione di liceità assai diversa dalle altre e, soprattutto, giocoforza residuale, benché il suo uso attuale nella prassi possa creare delle illusioni ottiche e farla sembrare prioritaria: e, infatti, va ribadito che del consenso vi è necessità solo quando mancano altre basi (peraltro, come oltre si dirà, tale priorità logica dovrebbe tradursi anche in una preminenza deontologica, nel senso che, ove vi è spazio per altre basi, il titolare del trattamento non dovrebbe ricorrere al consenso o comunque dovrebbe essere disincentivato a fare ricorso ad esso).

privacy, quanto alla limitazione di altri diritti, quale quello all'autodeterminazione commerciale); né hanno contezza del valore che i loro dati personali rivestono per le controparti (sicché sono portati ad accettarne la dismissione anche senza riceverne una vera e propria utilità in cambio). Per di più, spesso gli utenti suppongono che i loro dati sono già in circolazione che, quindi, non potendo più esercitare un controllo sugli stessi, risulta indifferente ammettere nuovi e ulteriori trattamenti.

Questi fenomeni possono venire raccolti sotto l'ampia dicitura di *privacy paradox*[9]: tanto più importante è la protezione dei dati in una società che evolve, tanto meno è, da un lato, strutturalmente attuabile tramite condotte dei singoli e, da un altro lato, avvertita e percepita come tale da questi stessi singoli. Potremmo, convenzionalmente, definire il primo ambito del "paradosso dell'attenzione" e il secondo del "paradosso della valutazione": il primo dipende dall'asimmetria del tempo tra chi tratta i dati e chi li fornisce, tale per cui al secondo non può essere richiesta la lettura analitica delle condizioni del trattamento; il secondo, invece, dalla mancanza di una cultura diffusa in tema di dati, sicché il loro trattamento non è – in breve – sentito come minaccia a certi valori.

Tali paradossi, ovviamente, rendono il consenso al trattamento dei dati una base potenzialmente distruttiva rispetto al sistema: da un lato, è ovvio che, se non perimetrato entro confini rigidissimi, il consenso fornito dall'interessato potrebbe fisiologicamente non corrispondere a una scelta reale o comunque a una scelta realmente ponderata; da un altro lato, è altrettanto evidente che, in tali situazioni, chiedere e ottenere il consenso al trattamento può costituire una facile scappatoia rispetto al sistema di liceità del trattamento.

Quest'ultima considerazione è tanto più vero, quanto più spesso avviene che i singoli forniscano il loro consenso (anziché rifiutarlo). Ma, a ben vedere, essa resta vera anche se statisticamente assenso o

---

[9] Cfr. S.B. Barnes, *A Privacy Paradox: Social Networking in the United States*, in *First Monday*, 2006. Alcune specificazioni di questo paradosso sono fornite da: S. Trepte. - D. Teutsch - P.K. Masur - C. Eicher - M. Fischer - A. Hennhöfer - F. Lind, *Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS)*, in S. Gutwirth, R. Leenes e P. de Hert (a cura di), *Reforming European Data Protection Law*, Dordrecht-Heidelberg-New York, 2015, p. 333 ss.; D.J. Solove, *Introduction: Privacy Self-Management and The Consent Dilemma*, in *Harvard Law Review*, 2013, p. 1881 ss.; Id., *"I've Got Nothing to Hide" and Other Misunderstandigs of Privacy*, in *San Diego Law Review*, 2007, p. 745.

diniego si equivalgono e perfino se il rifiuto supera statisticamente il consenso: e, ciò, perché comunque la condizione di liceità *consent-based*, se non rigidamente regolata, non assicura la presenza di una volontà vera o comunque veramente ponderata nemmeno nei (pochi o statisticamente meno numerosi) casi in cui essa si presenta, finendo anzi per ridursi a una trappola per utenti inesperti da schivare[10].

Senza dire che nemmeno di fronte a un (fisiologico) rifiuto generalizzato al trattamento potremmo dirci appagati. Se, infatti, il rifiuto non deriva da un atto di volontà (vera e veramente ponderata), esso di per sé si accompagna a delle criticità: può accadere, infatti, che esso si ritorca contro gli stessi interessi del titolare dei dati, che avrebbe avuto convenienza ad accettare il trattamento, e di riflesso che pregiudichi proprio il titolare del trattamento. Il risultato sarà, inevitabilmente, l'inefficacia del sistema del consenso (assieme a un inevitabile pregiudizio di quel *free flow of personal data*, che tanto sta a cuore al legislatore eurounitario e più in generale all'economia moderna).

E, ancora, un simile rifiuto generalizzato finisce per rendere l'utente una sorta di burocrate, costretto a muoversi tra svariate richieste, che per il contesto in cui sono formulate spesso richiedono di venire lette quanto meno nelle prime parole, per poi essere pedissequamente rifiutate[11].

---

10 Del resto, spesso non vi è alcuna ragione per il titolare dei dati a dare il suo consenso; eppure, benché manchi tale interesse, il consenso viene prestato. Giacché le ipotesi in cui il *data subject* vuole consapevolmente arricchire la sua controparte, concedendole l'uso dei suoi dati, sono giocoforza limitate, è evidente che l'autorizzazione al trattamento finisce per essere un feticcio che non corrisponde ad alcuna volontà reale.

11 Le ultime ragioni indicate rendono, a mio avviso, poco credibile che un semplice incremento della "cultura dei dati" (pur auspicabile) possa risolvere tutti i problemi regolatori attualmente sussistenti. E, infatti, per quanto sia da guardare con favore quel cambio antropologico che porterà – così si crede o per lo meno si spera – a rendere i dati (la loro protezione e il loro trattamento) veri e propri valori, avvertiti socialmente e socio-giuridicamente e non solo disciplinati come tali dall'interno dell'ordinamento giuridico (in virtù dei riflessi che l'utilizzo dei dati personali inevitabilmente ha), comunque anche tale mutamento non escluderebbe i problemi legati al paradosso dell'attenzione e alla correlata necessità, per l'utente che vi si volesse sottrarre, di trasformarsi in un burocrate, continuamente raggiunto da richieste di consenso da leggere e valutare.

6.3. Regolazione e interpretazione del consenso, oggi

Già nelle disposizioni dedicate alle condizioni di liceità del trattamento il consenso, oltre a venire menzionato, trova alcuni cenni di disciplina: all'art. 6 si prevede che il consenso vada fornito "per una o più specifiche finalità"; all'art. 9 si aggiunge che esso, se relativo a dati "di categorie particolari", sia anche "esplicito".

Tuttavia, è soprattutto negli art. 4(11) e 7-8 che il consenso viene regolato. Ivi, in particolare, si definisce il consenso dell'interessato quale "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". Inoltre, si stabilisce che l'onere della prova del consenso sia a carico del titolare del trattamento; che, nel consenso di consenso prestato nel contesto di una dichiarazione scritta più ampia, la sua richiesta sia chiaramente distinguibile, comprensibile, facilmente accessibile; che la libertà del consenso debba essere valutata tenendo "nella massima considerazione l'eventualità … che l'esecuzione di un contratto … sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto". L'art. 8, poi, detta ulteriori condizioni riguardanti il "consenso dei minori in relazione ai servizi della società dell'informazione".

A lato, v'è anche da menzionare la Direttiva *ePrivacy* (volgarmente detta *cookie law*), ossia la Direttiva 2002/58/CE, la quale prevede quale unica base per il trattamento dei dati personali rientranti nel suo ambito di applicazione (e, quindi, in particolare i *cookie*[12]) il consenso dell'interessato. Consenso che, peraltro, "corrisponde al consenso della persona interessata di cui alla Direttiva 95/ 46/CE" (così l'art. 2, lett. f])[13].

Al fine di comprendere come debbano venire intese tali disposizioni appaiono della massima utilità, per la loro intrinseca condivisibilità, così come per la loro autorevolezza, le linee guida elaborate di

---

[12] Sulla profilazione mediante uso di *cookie* e strumenti simili v. oggi anche le Guidelines 8/2020 on the targeting of social media users, version 1.0., adopted on 2 September 2020.

[13] Oggi v. l'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019.

recente dall'European Data Protection Board e che aggiornano e completano le linee guida del Gruppo di lavoro Articolo 29[14].

La "libertà" del consenso manca, secondo l'EPDB, se il soggetto è costretto di fatto a dare il suo consenso perché intende ottenere un bene o un servizio o perché il rapporto in cui agisce è fortemente squilibrato.

Il primo gruppo di casi richiama le cosiddette *tying practices*[15], rispetto alle quali il GDPR mantiene una posizione abbastanza equivoca all'art. 7, par. 4, e al considerando 43[16]: probabilmente, incrociando le varie tesi sostenute, allo stato deve ritenersi che la necessità di prestare il consenso per accedere a beni o servizi essenziali lo renda inevitabilmente invalido e che, invece, là dove si tratti di beni o servizi non essenziali il consenso possa essere validamente richiesto e prestato, purché ciò avvenga con modalità tali da far dubitare della libertà del consenso[17]. Ad esempio, sarebbe ammesso condizionare uno sconto al consenso; non, invece, condizionare l'accesso a una *app* già scaricata al

---

14 Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1., adopted on 4 May 2020.

15 Su cui molto si è scritto di recente: v. per tutti A. De Franceschi, *La circolazione dei dati personali tra* privacy *e contratto*, Napoli, 2017; C. Langhanke e M. Schmidt-Kessel, *Consumer Data as Consideration*, in *Journal of European Consumer and Market Law*, 2015, p. 218 ss.

16 Secondo cui, rispettivamente, va tenuta nella "massima considerazione" l'eventualità che l'esecuzione del contratto sia condizionata al consenso, "presumendosi" la mancanza di libertà se il trattamento dei dati non è necessario per tale esecuzione.

17 Sulla prima ipotesi v. l'*Handbook on European Data Protection Law*, Luxembourg, 2014, p. 58 (che parla, a dire il vero, di beni "sufficientemente importanti"); sulla seconda, in realtà, le Guidelines 05/2020 sostengono una tesi abbastanza restrittiva, secondo la quale la libertà mancherebbe ogni qual volta un servizio fosse richiesto verso la controprestazione di dati, anche se nel mercato fosse possibile reperirlo verso una controprestazione in denaro. Nondimeno, parrebbe lecito subordinare al consenso l'ottenimento di uno sconto, giacché in tal modo sarebbe ben chiara all'interessato la scelta che compirà concedendo il suo consenso. Le due ipotesi divergono, come meglio diremo oltre, poiché la prima si avvicina di più a una costrizione, la seconda a una influenza indebita. Resta qualche dubbio per il caso di iscrizione a una *newsletter*, ove non si può ritenere che il trattamento avvenga sulla base della necessità contrattuale, poiché lo stesso trattamento costituisce (di regola) remunerazione per il *data controller*; in tal caso appare ragionevole costruire il consenso quale negozio collegato che fornisce la controprestazione, a sua volta inserita in uno schema di scambio condizionale (cfr., sullo scambio di dati personali a fronte dell'iscrizione a una *newsletter*, Cass. civ., Sez. I, 2 luglio 2018, n. 17278, in *NGCC*, 2018, I, p. 1775).

consenso a un trattamento di dati non direttamente necessario per la stessa prestazione del servizio[18] o l'accesso a una pagina internet al consenso ai *cookie*, come avviene tramite i cosiddetti *cookie walls*[19].

Il secondo gruppo di casi richiama situazioni in cui il *data subject* versa in posizione di debolezza verso il titolare del trattamento, tanto da essere portato di fatto ad acconsentire al trattamento, senza poter esercitare una libera scelta. Si tratta, ad esempio, dei casi del lavoratore rispetto al suo datore o del privato verso un'autorità pubblica[20].

Sotto un punto di vista diverso, la "libertà" del consenso, e quindi l'"effettività" del volere, difetta se il consenso viene richiesto per un insieme di scopi, anziché "granularmente" per singoli e specifici scopi (come, del resto, confermano anche i considerando 32 e 43[21]).

Tale requisito si collega, poi, a quello della "specificità" del consenso, che di nuovo mira a garantire l'"effettività" del volere: il consenso deve venire prestato in relazione a uno o più scopi specifici, stabiliti anticipatamente dal titolare del trattamento. Del resto, è un principio generale, espressamente stabilito dal GDPR, quello per cui gli scopi del trattamento debbono essere già decisi prima della raccolta dei dati (cfr. art. 5, par. 1, lett. b])

La specificità, a sua volta, ci porta a considerare quello dell'"informazione": per ciascuno degli scopi specifici del trattamento basato sul consenso, ossia per ciascuno dei singoli atti di consenso che vengono richiesti, l'interessato deve essere sufficientemente informato.

L'informazione ha un contenuto minimo, desumibile in parte dei considerando, in parte dalle previsioni del GDPR, in parte da un'interpretazione sistematica e funzionale del testo di legge[22]. Secondo

---

18 In tal caso, peraltro, la base più appropriata per il trattamento sarebbe quella indicata nell'art. 6, par. 1, lett. b. Sulla pratica, molto comune, dei titolari del trattamento di munirsi del consenso anche ove vi è una diversa base per il trattamento v. *infra*.

19 Connesso al requisito in parola è quello della mancanza di pregiudizio (*detriment*), in base al quale il titolare del trattamento deve poter dimostrare che il rifiuto o la revoca del consenso non porta a costi o a svantaggi per il titolare dei dati (v. anche il considerando 42).

20 V. anche qui il considerando 43.

21 Secondo cui, rispettivamente, il consenso deve essere dato per tutti gli scopi di un trattamento, fermo restando che esso non è libero se non si permette al *data subject* di acconsentire separatamente a diverse operazioni di trattamento dei dati.

22 V., quanto al testo del GDPR, il considerando 42 e l'art. 7, par. 3.

l'EDPB, tale contenuto coincide – tra l'altro – con l'identità del titolare del trattamento, lo scopo di ciascuna operazione di trattamento, il tipo di dati raccolti e usati, il diritto di revocare il consenso.

Ancora più importante, però, è chiedersi come vanno fornite le informazioni, anche al fine di rispettare il principio di trasparenza e di permettere al *data subject* di porre in essere una decisione consapevole (il che, a ben vedere, ridonda ancora una volta nell'"effettività" del volere[23]). In ogni caso, la richiesta di consenso – che è il mezzo comune con cui il titolare del trattamento cerca di ottenere il consenso e che, soprattutto, è un mezzo sicuramente ammesso dal GDPR – deve essere redatta in modo chiaro e con linguaggio semplice, comprensibile ai presumibili destinatari della comunicazione[24]. È opportuno, inoltre, che le informazioni siano fornite in modo breve e conciso: a tal riguardo il titolare del trattamento si può servire di una costruzione a più livelli (*layered*), fornendo al primo livello alcune informazioni basilari e, poi, rinviando ad altre pagine per l'indicazione di dettagli via via più specifici[25].

Infine, l'atto di consenso deve risultare "non ambiguo", risultando altrimenti dubbia la presenza di una volontà "effettiva". In linea generale, si prescrive che il consenso sia prestato tra un "atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano" (così il considerando 32).

Più nel dettaglio, il GDPR (allo stesso considerando) specifica che, per quanto non vi siano oneri di forma particolari (sono possibili dichiarazioni scritte, anche con strumenti elettronici, o pure orali), non possono essere considerati validi atti di consenso il silenzio, le caselle

---

23 Insiste sulla consapevolezza "del fatto" e "della misura" il considerando 42.

24 Ai sensi dell'art. 7, par. 2, sembrerebbe che ciò sia richiesto solo laddove la richiesta di consenso sia parte di una dichiarazione scritta più ampia. In realtà, il requisito in parola ha una portata assai più estesa; semmai, nel caso in cui la richiesta sia parte di una dichiarazione più ampia, il GDPR prescrive anche che essa sia facilmente distinguibile e accessibile. V., del resto, il considerando 32.

25 In tal modo, scrive l'EPDB, si possono al tempo stesso rispettare i doveri – apparentemente contrastanti – di precisione e completezza, da un lato, e di semplicità, dall'altro.

pre-spuntate[26] o la semplice inattività; al contrario, possono esserlo le spunte di caselle durante la visita di una pagina *web* o anche semplicemente la scelta di impostazioni tecniche per i servizi della società dell'informazione (ad esempio, la scelta di impostazioni di un *browser*). Per l'effetto, non si può ad esempio considerare valido il consenso ai *cookie* prestato semplicemente continuando la navigazione in una pagina internet.

Per quanto riguarda i soli dati di cui all'art. 9 GDPR, il consenso dev'essere anche "esplicito": a tal fine, può consistere in una dichiarazione scritta e firmata, ma può essere sufficiente anche il riempimento di un modulo *online*, una *email* o l'*upload* di un documento firmato. Anche la forma orale potrebbe essere idonea; tuttavia, la necessità che il titolare del trattamento provi l'esistenza di tutte le condizioni richieste per il consenso esplicito rende assai difficile che questi si accontenti di una dichiarazione orale (tutt'al più, si possono immaginare dichiarazioni telefoniche registrate, ammesso che si riesca a provare in tal modo anche di aver fornito informazioni sufficienti in un modo chiaro, adeguato e trasparente).

Con riguardo a qualsiasi categoria di dati personali, il considerando 32 e l'art. 7, par. 3, prevedono anche che, quando la richiesta di consenso avviene tramite mezzi elettronici, la richiesta non deve "interferire immotivatamente con il servizio per il quale il consenso è espresso" e che la revoca del consenso deve essere tanto facile quanto la sua concessione. Tali disposizioni potrebbero avere un riflesso assai importante sul modo in cui viene ricostruito il consenso (e non solo la revoca); tuttavia, esse vengono a tutt'oggi per lo più intese in senso letterale: la prima, come volta a evitare fastidi nella navigazione sui siti (sicché il consenso, pur richiedendo un atto positivo e non ambiguo, non dovrebbe essere eccessivamente difficile da prestare) e, la seconda, come volta a regolare unicamente le modalità della revoca. Su questi punti torneremo comunque oltre.

6.4. Forza e debolezza dell'approccio attuale

Come si è visto, la tendenza dell'ordinamento eurounitario è nel senso di creare dei confini al trattamento dei dati, onde renderlo il più

---

[26] Cfr. Corte di Giustizia, 11 novembre 2020, C-61/19; v. anche Corte di Giustizia, 1 ottobre 2019, C-673-17, per il caso di caselle pre-spuntate e *cookie*.

possibile informato e libero. Tuttavia, restano probabilmente dei problemi, che l'approccio attuale non riesce a superare.

Per descrivere i punti di forza e di fragilità dell'attuale sistema, è necessario ampliare la prospettiva.

Qualsiasi sistema o sottosistema che si basi sulla volontà individuale non può, per forza di cose, richiedere un accertamento circa la presenza di una volontà psichica perfettamente formata di chi dichiara il suo volere. Nondimeno, il sistema può funzionare perché, di norma (fisiologicamente), chi dichiara il suo volere effettivamente ha posto in essere una scelta coincidente, sufficientemente ponderata almeno nei suoi elementi centrali[27].

E, difatti, solo se così è si può addebitare a un soggetto, in ragione della sua autoresponsabilità, una dichiarazione che (patologicamente) non corrisponde alla sua volontà. Questo è quanto avviene, di regola, nel sistema dei contratti, in cui chi dichiara sa o può sapere a cosa va incontro.

Più specificamente, chi dichiara è o può essere perfettamente consapevole degli elementi centrali del contratto, mentre per quelli di minore rilievo può ben demandare la disciplina, se non vuole interessarsene, all'ordinamento giuridico (confidando sul fatto che tale disciplina sarà la più equilibrata possibile). E lo stesso vale finanche dove ci si allontani dal sistema del codice civile, per approdare al contratto del consumatore: anche in tal caso, infatti, il contraente debole può scegliere l'*an* del contratto e può sindacarne i profili essenziali (bene o servizio, prezzo); quanto, invece, alla disciplina ulteriore, è proprio la fisiologica impossibilità di averne contezza (unitamente all'altrettanto fisiologica impossibilità di farne oggetto di trattativa) a consigliare un intervento correttivo da parte dell'ordinamento giuridico[28].

---

27 Rispetto a questa fisiologia possono ben sussistere situazioni patologiche, le quali tuttavia sono, per l'appunto, patologiche: si pensi, per il caso del contratto, al sistema dei tradizionali vizi del volere (errore, dolo, violenza, incapacità).

28 Patologia diversa è quella che emerge là dove un soggetto non sia in condizione di decidere l'*an* del contratto e si trovi quindi soggetto al potere altrui: si pensi ai casi di monopolio, oligopolio e anche, nell'ambito del terzo contratto, all'abuso di dipendenza economia. Simile, inoltre, è la condizione del soggetto vulnerabile: colui che, cioè, è portato – a causa della sua condizione o in ragione di un'influenza indebita di controparte – a concludere un certo contratto.

Il sistema del consenso al trattamento, tuttavia, non rispetta questi principi. In quei casi, infatti, la patologia diviene la normalità: è normale che chi presta il suo consenso non abbia piena contezza di quanto sta facendo. A fronte di ciò, l'ordinamento dovrebbe necessariamente ripristinare, tramite un suo intervento, l'effettività del consenso: in caso contrario il sistema non può funzionare o, comunque, finisce per essere inefficace.

L'ordinamento, a sua volta, può agire in astratto in due forme diverse: rendendo fisiologicamente reale il consenso; correggendo, sulla base degli interessi normali del titolare dei dati, la disciplina specifica del trattamento.

Il primo approccio è quello per lo più scelto a livello europeo. La ragione è di ordine logico: il consenso al trattamento attiene per lo più a una scelta su un elemento centrale, rispetto a cui è difficile supporre che un terzo possa, per quanto sulla base di un interesse normale della parte, sostituirsi (si finirebbe, di fatto, per sostituire al consenso una diversa condizione di liceità, vagamente corrispondente al legittimo interesse)[29]. Soltanto di fronte a una esorbitante mancanza di interesse in capo al *data subject* oppure per quanto attiene al *quomodo* del trattamento – il cui rilievo, però, è assai limitato – si può pensare a un intervento correttivo fondato sull'interesse normale del titolare dei dati (i rischi corsi e i benefici ottenuti, entrambi valutati secondo normalità e ragionevolezza).

In questo quadro possiamo allora inserire gli interventi regolatori di cui s'è detto nel precedente paragrafo: quando richiedono un consenso informato e libero, in realtà il più delle volte cercano di superare il *privacy paradox*, rendendo vera e veramente ponderata la volontà.

---

[29] E, infatti, in questo caso mancherebbe un criterio interno alla stessa pattuizione (proprio perché la verifica riguarderebbe un elemento centrale della pattuizione, che giocoforza non potrebbe essere al tempo stesso oggetto della valutazione e parametro della stessa; al contrario, laddove la verifica riguarda elementi accessori, è ovvio che la si può compiere sulla base di quell'economia interna allo stesso contratto). Il criterio esterno, su cui inevitabilmente basarsi, non sarebbe che quello dell'interesse "normale" a dare i dati: con la conseguenza che l'atto di consenso verrebbe pienamente materializzato e la volontà a sua volta totalmente compressa. Il consenso, così, lascerebbe di fatto spazio a un bilanciamento tra gli interessi del titolare del trattamento e i rischi (e gli interessi) del titolare dei dati; per l'effetto, si tradurrebbe in una sorta di legittimo interesse.

Così, la necessità di un consenso specifico (granulare), non inglobato in un testo contrattuale, dovrebbe assicurare che sia prestata attenzione a tutti i possibili trattamenti; inoltre, il dovere di informare chiaramente, in modo accessibile e breve (e con la necessità di rinviare ad altri testi per ulteriori spiegazioni), dovrebbe garantire circa l'esistenza dei presupposti di una scelta reale; l'esigenza di lasciare libero il consenso, evitando di subordinare l'accesso a siti allo stesso, dovrebbe tra l'altro scongiurare il rischio di una decisione frettolosa[30].

Al contrario, la valutazione di impatto preventiva può leggersi nel secondo ambito: l'art. 35 GDPR, infatti, nel prevedere che in determinati casi il titolare del trattamento sia tenuto a svolgere una tale valutazione, parrebbe implicarne un possibile esito negativo, con conseguente preclusione del trattamento previsto. Una simile interpretazione è peraltro confortata dalla lettura dell'art. 36 GDPR, che in tema di consultazione preventiva dell'Autorità di controllo non esclude affatto la possibilità che quest'ultima esprima parere negativo al trattamento, per l'assenza di misure adottate (anche se corrispondenti a tutte quelle adottabili) idonee ad attenuare sufficientemente i rischi[31].

Questi interventi senza dubbio debbono essere visti con favore, poiché essi percorrono una strada volta a superare i problemi indicati in

---

30 Anche il consenso al trattamento può mancare di libertà sotto un altro e diverso punto di vista, simile a quello di cui s'è detto nella precedente nota: allorché il consenso al trattamento è necessario per ottenere un bene o un servizio essenziale, ecco che viene a mancare la necessaria libertà. Escluderei, però, che nel caso di accesso a un sito qualunque si possa parlare di un bene o di un servizio essenziale: sicché la garanzia di libertà deve, in tali casi, essere riletta nel senso di cui al testo. Inoltre, un'analoga patologia potrebbe presentarsi ogni qual volta un soggetto non è in condizione di decidere serenamente sull'autorizzazione al trattamento: non tanto perché non ne ha il tempo o non è in grado di comprendere i valori alla base, ma perché, per la specifica situazione in cui opera, non può scegliere in modo libero. Conseguentemente, anche questi casi in effetti possono comportare un problema di libertà (si tratta, in particolare, delle già menzionate ipotesi in cui tra le parti vi è un rapporto asimmetrico e di dipendenza, come quello tra privato e autorità pubblica o tra dipendente e datore di lavoro).

31 Sulla valutazione d'impatto preventiva v. per tutti E. BATTELLI e G. D'IPPOLITO, *Art. 35 RGPD*, in *Comm. Gabrielli*, Milano, 2019, p. 661 ss.

apertura[32]. Tuttavia, forse essi non sono ancora sufficienti ad assicurare il pieno funzionamento del sistema del consenso.

Il punto richiederebbe indagini d'ordine psicologico e comportamentale[33]: nondimeno, già in via di prima approssimazione, e sulla base della comune esperienza, si può notare come, nonostante una consapevolezza generale che aumenta e che sempre più conduce le persone a ritenere "importanti" i loro dati[34], i paradossi cui si è fatto riferimento – il paradosso dell'attenzione e quello della valutazione – aleggiano ancora sul consenso al trattamento, con tutto ciò che ne consegue.

Pensiamo, anzitutto, al caso dei *cookie*.

È evidente che, là dove la scelta proposta dal gestore di un sito è tra accettare tutti i *cookie* o selezionare quelli davvero voluti, essa diviene di fatto irreale, poiché nessuno o quasi nessuno avrà il tempo per scegliere, per ciascun sito, i *cookie* ammessi[35]. Là dove, invece, è presente anche un pulsante di rigetto di tutti i *cookie* (o comunque, in assenza di scelta, il gestore del sito non installa altri *cookie* se non quelli tecnici), i problemi diminuiscono ma non sono del tutto evitati, giacché – di nuovo – è ovvio che nella normalità dei casi l'utente accetterà o rifiuterà tutto, in blocco; e lo farà sulla base per lo più di una personale posizione generale circa il tema della protezione dei dati (indifferenza o preoccupazione per i propri dati[36]), tutt'al più ammorbidita a se-

---

32 Seguendo un'opinione già sostenuta da Simitis, B. Buchner e J. Kühling, *Art. 7 DS-GVO*, in *DS-GVO - BDSG Kommentar*[2], München, 2018, p. 289 s., sostengono che in passato il consenso spesso non era che una "bloße Fiktion"; oggi il GDPR, secondo i due autori, cerca di circoscrivere l'ammissibilità del consenso proprio nei casi in cui esso ridonda in una finzione.

33 Indagini che, del tutto opportunamente, iniziano a venire compiute: v., a proposito uno studio condotto presso l'Università Suor Orsola Benincasa, I.A. Caggiano, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica studi comportamentali*, in *ODCC*, 2018, p. 67 ss.

34 La diffusione di una "cultura dei dati" è uno degli obiettivi del GDPR, che probabilmente verrà raggiunto, e in parte è stato già conseguito, anche grazie all'insistenza sui diritti del singolo e sulla rigida regolazione del consenso al trattamento.

35 Come si sul dire, utilizzando un'espressione emblematica, la scelta è eccessivamente *time-consuming*.

36 Peraltro, l'utente indifferente, al solo fine di togliere dalla vista il *banner* dei *cookie*, potrebbe cliccare su "accetta" solo per un riflesso incondizionato (perché "accettare"

conda dei connotati apparenti del sito (ad esempio, se il gestore sembra affidabile e il sito interessante, si potrà pensare di accettare l'installazione dei *cookie*).

Ma anche al di fuori dei *cookie* si presentano numerosi problemi: un soggetto normale, mediamente diligente, spesso non è in condizione di compiere una scelta reale, mancando di tempo o comunque di facoltà cognitive sufficienti per porre in essere singole decisioni ponderate[37].

Ad esempio, a fronte di varie caselle relative al trattamento dei dati, non preselezionate, la prima delle quali riguarda un trattamento necessario per l'esecuzione di un contratto (rispetto a cui però il titolare chiede il consenso, non accontentandosi della diversa e apposita base legale) e le altre invece si riferiscano a trattamenti per finalità in senso lato pubblicitarie, avviene spesso che l'utente le rifiuti tutte o, al contrario, le accetti tutte, fermandosi a leggere solo la prima e poi compiendo istintivamente una medesima selezione per tutte le caselle o ipotizzando che sia necessario acconsentire per poter ottenere il bene o il servizio che, poniamo, in quel momento si sta acquistando.

E questa situazione è comune – e quindi, per così dire, "patologicamente fisiologica" – anche là dove i singoli trattamenti sono indicati in modo semplice, con frasi concise e con rimando (secondo una struttura "a più livelli") ad altri documenti per i necessari approfondimenti: anzi, in tal caso si pongono ulteriori problemi, ogni qual volta la richiesta di primo livello, nella sua necessaria brevità, non dà conto esattamente del trattamento e non permette, quindi, di compiere una decisione veloce e al tempo stesso sufficientemente consapevole.

---

a prima vista pare più positivo e sbrigativo di "rifiutare", anche se poi in realtà il "rifiuto" sarebbe equivalente). Lo stesso utente indifferente potrebbe acconsentire al trattamento ritenendo tendenzialmente preferibile, in termini generali, l'utilizzo dei suoi dati, piuttosto che il mancato utilizzo. L'utente preoccupato per l'uso dei suoi dati potrebbe compiere una scelta opposta, ma sempre non riflettuta. Del resto, anche un utente particolarmente attento difficilmente perderebbe tempo per scegliere i *cookie* che trova davvero utili, selezionandoli uno ad uno; piuttosto, deciderebbe se acconsentire o meno sulla base di una scelta semplicistica (favorevole, se uno o più *cookie* sono probabilmente utili; sfavorevole, in caso contrario).

37 In linea generale, si è notato che, mentre per i dati sensibili il consenso spesso è davvero informato e libero, per gli altri dati esso si riduce di regola a una veloce spunta di una casella. Cfr. B.-J. Koops, *The Trouble with European Data Protection Law*, in *International Data Privacy Law*, 2014, p. 251 ss.

E i problemi non derivano solo dalla scarsità di tempo e facoltà cognitive dell'interessato: talvolta, infatti, essi si collegano all'impossibilità, per un soggetto medio, di valutare i rischi e i benefici per le parti connessi al trattamento.

Ad esempio, una società sviluppatrice di *software*, che chiedesse semplicemente il consenso a inviare *report* dei *crash* di una sua applicazione, con tutta probabilità non chiarirebbe i menzionati rischi e benefici: ossia, per il *data subject*, il rischio di un *data breach* o comunque di un uso illecito dei suoi dati e, all'opposto, per il *data controller*, il beneficio derivante dal trattamento.

In breve, accade ancora spesso che la decisione sul consenso non abbia fisiologicamente modo di essere davvero consapevole e meditata: tra condizionamenti esterni (in particolare, la necessità di approvare per non perdere tempo o di rigettare per evitare rischi, così come l'impossibilità di prendere visione compiutamente di tutte le specifica finalità dei trattamenti) e difficoltà interne (soprattutto inerenti alla complessità che ogni valutazione dei rischi porta con sé), essa finisce per risultare inidonea a veicolare una normale volontà (ossia una volontà che, salvo fattori patologici, è presente).

E, di qui, una prima conseguenza: il disallineamento tra quello che sarebbe un consenso pieno e quello che invece è il consenso oggi rende ancora ipocrita questa base del trattamento, allorché essa è presente. Né si potrebbe invocare, in questi casi, l'autoresponsabilità del singolo: tale principio, come si è detto, può avere un valore per addebitare a ciascuno di noi le conseguenze negative delle sue azioni là dove sia normale e fisiologico che un soggetto mediamente diligente le eviti; non, invece, qualora sia inevitabile o comunque assai probabile che finanche l'uomo comune (un tempo si sarebbe detto: *bonus paterfamilias*) vi vada incontro. Per l'effetto, il modello di diligenza che si vuole adottare va plasmato sulle particolarità del contesto, tenendo peraltro in considerazione che, più lo si rafforza, più si finisce per lasciare senza tutela proprio i soggetti che ne sarebbero più bisognosi, mentre, più lo si indebolisce, più si tutela il contrario interesse di chi vorrebbe trattare i dati personali.

E non è tutto: le conseguenze, come già accennato, sono anche altre. Là dove manca il consenso, non è detto che sia compiuta una scelta (reale e ponderata): sì che l'assenza del consenso non è indice della mancanza di un interesse del *data subject* o, comunque, di un bilanciamento posto in essere, anziché dall'ordinamento, da quest'ultimo. E,

comunque, in tali casi si deve anche tenere in considerazione il disturbo inevitabilmente arrecato al titolare dei dati, ogni qual volta la richiesta interrompe la navigazione o comunque richiede la sua attenzione, anche solo per un istante e per negare – il più delle volte senza nemmeno leggere l'intero testo della richiesta, anche se sintetizzato in poche righe – il suo consenso.

A fronte di tutto questo, ci si deve chiedere se il consenso può essere reso maggiormente effettivo, senza con ciò comprimere eccessivamente gli interessi – legittimi – dei titolari del trattamento. E la risposta richiede, anzitutto, di domandarsi se un aiuto in questo senso può derivare dall'inquadramento dogmatico del consenso e, in senso luogo, di verificare se, indipendentemente da questo, una revisione ermeneutica o una riforma legislativa dei requisiti del consenso possa portare nella direzione divisata.

6.5. L'inquadramento dogmatico: una prima proposta (priva di effettiva utilità)

Come noto, l'inquadramento dogmatico del consenso al trattamento ha visto contrapporsi – in Italia come all'estero – opinioni anche assai distanti: in particolare, mentre taluni autori hanno accolto tesi negoziali (o addirittura contrattuali), altri hanno ridotto il consenso al trattamento ora (in Italia) a un atto giuridico in senso stretto, ora (in Germania, ossia nell'ordinamento dove maggiormente si è studiato l'inquadramento dogmatico dell'*Einwilligung*) a un atto pseudo-negoziale o a un atto reale[38].

Ciò che accomuna queste opinioni, come si sarà inteso, è il loro radicamento nell'ordinamento italiano: ossia, l'applicazione della dogmatica italiano all'atto di consenso. Nel vigore del GDPR, tuttavia, può per lo meno dubitarsi della correttezza di quest'operazione: sia perché esso è un Regolamento (e tende quindi all'uniformità del diritto), sia perché esso disciplina in modo pressoché compiuto l'atto di consenso,

---

[38] Per una sintesi delle diverse posizioni sostenute in Italia v. S. THOBANI, *I requisiti del consenso al trattamento dei dati personali*, Santarcangelo di Ramagna, 2016, p. 2 ss. Per quelle tedesche v. invece P.M. ROGOSCH, *Die Einwilligung im Datenschutzrecht*, Baden-Baden, 2013, p. 36 ss.

sì che l'interpretazione (anche quella sistematica) dovrebbe essere condotta su un piano eurounitario, e non interno[39].

A fronte di ciò, però, è facile accorgersi che la mancanza di categorie eurounitarie rende assai difficile l'inquadramento dogmatico dell'atto di consenso: si tratta di un primo fattore che, già a livello generale, depone per l'inutilità dell'operazione di qualificazione, a fronte dell'assenza, a livello di diritto UE, di una teoria generale del negozio (e del contratto) e, viceversa, della presenza, nel GDPR, si una disciplina specifica per l'atto di consenso.

Tuttavia, possiamo provare a mettere da parte lo scetticismo e verificare se l'inquadramento dogmatico eurounitario può essere di una qualche utilità per risolvere i nostri problemi.

6.5.1. L'inquadramento generale

Possiamo definire – secondo una rivisitazione della dottrina pandettistica, che in vario modo ha influenzato l'intera tradizione di *civil law* – i meri atti quali dichiarazioni o comportamenti la cui regolazione coincide in tutto e per tutto con il loro significato socio-giuridico intrinseco e fattuale (venendo dunque disciplinati da una *regulative rule*) e i negozi quali atti che pongono una regola la quale, di per sé, non si riduce al significato socio-giuridico intrinseco e fattuale della dichiarazione o del comportamento, ma costituisce il frutto dell'attivazione concreta di una convenzione socio-giuridica direttamente volta ad approvare di una regola (il frutto dell'attivazione concreta di una *constitutive rule*)[40].

Quanto al consenso al trattamento, l'inquadramento come mero atto impone di ritenere che il permesso di utilizzare i dati crea una regola già immanente all'atto; quello, invece, come negozio richiede di

---

[39] A favore della necessità di un inquadramento eurounitario e autonomo v. F. Bravo, *Il consenso*, cit., p. 157 ss., e già G. Alpa, *La disciplina dei dati personali*, Roma, 1998, p. 90; nella letteratura tedesca v. A. Ingold, *Artikel 7*, in *Europäische Datenschutzgrundverordnung - Handkommentar*[2], Baden Baden, 2018, p. 450. Per la possibilità di utilizzare categorie interne, onde utilizzare per l'atto di consenso la disciplina interna quanto meno in via residuale (laddove la disciplina eurounitaria lasci aperti degli spazi), v. G. De Cristofaro, *Die datenschutzrechtliche Einwilligung als Gegenstand des Leistungsversprechens*, in T. Pertot (hrsg.), *Rechte an Daten*, Tübingen, 2020, p. 158 ss.

[40] Si consenta il rinvio ad A.M. Garofalo, *Le regole costitutive del contratto*, Napoli, 2018. La differenza tra atto e negozio giuridico è nota anche ai progetti di *soft law*: v. art. II.-1:101(2) DCFR.

rinvenirvi un atto che, già per il suo significato socio-giuridico, veicola qualcosa d'ulteriore, non immanente all'atto stesso. Un simile interrogativo, a sua volta, rappresenta una questione difficile (un *hard case*) da risolvere dall'interno dell'ordinamento giuridico (ossia, sulla base della sistemazione e della specificazione dei valori sociali propria dell'ordinamento giuridico).

Tra gli argomenti che possiamo valorizzare, e che dall'interno del sistema giuridico ci aiutano a giungere a una soluzione, il più importante attiene all'inquadramento dogmatico dei dati personali in sé e per sé. Senza dilungarsi sulla questione, mi pare necessario ammettere che oggi i dati personali – là dove rilevanti[41] – rappresentino dei valori, nel senso che essi incarnano e rappresentano l'oggetto degli interessi (diversi) del titolare dei dati e del potenziale titolare del trattamento. Come tali, essi possono anche venire reificati[42], se non come beni in senso proprio quanto meno come oggetto di diritti contrapposti: da un lato, quello dell'interessato a vedersi riconosciuto, per l'appunto, come titolare dei dati, a respingere ogni trattamento illecito e a controllare ogni trattamento lecito; da un altro lato, quello del titolare del trattamento, a utilizzare un bene personale altrui ogni qual volta è presente una base per il trattamento[43].

---

41 Ossia, entro l'ambito oggettivo di applicazione del GDPR: cfr. art. 2. Al di fuori, e al netto delle diverse discipline nazionali, i dati personali non sono rilevanti in sé e per sé; l'attenzione del sistema giuridico (dei singoli sistemi giuridici) si sposta di regola sui singoli diritti e interessi che stanno a valle, senza attribuire rilievo autonomo ai dati personali.

42 Su questo tema cfr., da ultimo, C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, Torino, 2020. Sul dibattito, assai noto, circa l'ammissibilità di una "proprietà del dato", v. N. PURTOVA, *Property Rights in Personal Data: A European Perspective*, Alphen aan den Rijn, 2011; C. PRINS, *When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?*, in *Script-ed*, 2006, p. 270 ss.

43 Così ricostruito, il diritto del titolare del trattamento assomiglia a un diritto su cosa altrui, pur distinguendosene almeno sotto due profili: a) mentre i diritti reali su cosa altrui hanno consistenza prettamente patrimoniale, nel caso del diritto a utilizzare i dati le implicazioni per le due parti (interessato dal trattamento e titolare del trattamento) sono assai diverse e, soprattutto, sono differenti tra loro (v. *infra* nel testo); b) il diritto sui dati personali non è *erga omnes*, ma non è neppure un diritto relativo (è, piuttosto, un *pati* o, meglio ancora, l'attribuzione al titolare del trattamento di facoltà che, pur venendo ipostatizzate in uno specifico diritto, finiscono in realtà per ampliare le libertà generiche del titolare stesso). Sul dibattito, assai esteso in Italia, sui beni personali come beni immateriali oggetto di diritti v., da ultimo, la sintesi di

Ora, il consenso al trattamento, nel permettere l'utilizzo di questo bene, non è volto alla semplice rimozione di un limite e, soprattutto, non corrisponde a un'autorizzazione fattuale cui giuridicamente segue la disattivazione della di una certa disciplina (quella che proibisce il trattamento laddove difetti una base)[44]; piuttosto, il consenso al trattamento mira alla creazione, pur revocabile, di una situazione giuridica in capo a un altro soggetto[45]. E un simile effetto non è immanente alla fattualità della dichiarazione o del comportamento; esso, al contrario, deriva dall'attivazione di una convenzione socio-giuridica direttamente volta ad approvarlo. Di conseguenza, nell'atto di consenso deve rinvenirsi un negozio[46].

In replica non potrebbe sostenersi che tale inquadramento è disatteso dalla pratica sociale, in seno alla quale i dati personali ancora non

---

S. Thobani, *Diritti della personalità e contratto. Dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018, p. 51 ss.

44 L'autorizzazione fattuale (e in particolare la tolleranza, ma anche il consenso dell'avente diritto e secondo taluno anche altre ipotesi autorizzatorie) si esaurisce di per sé nel suo significato, che non è quello di approvare una modificazione della realtà deontologica, ma semmai quello di decidere interlocutoriamente e fattualmente circa l'utilizzo di un proprio bene (sì che i riflessi giuridici sono di stampo regolativo e non costitutivo, ossia non sono socialmente, socio-giuridicamente e giuridicamente l'oggetto verso cui direttamente si indirizza la volontà). Nel diritto italiano v., proprio con riferimento al consenso dell'interessato e con posizioni diverse, S. Patti, sub *art. 23*, in C.M. Bianca e D. Busnelli (a cura di), *La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196*, I, Padova, 2007, p. 553; G. Oppo, *Sul consenso dell'interessato*, in V. Cuffaro, V. Ricciuto e V. Zeno-Zencovich, *Trattamento dei dati e tutela della persona*, Milano, 1998, p. 124.

45 Nella dottrina tedesca, v. M. Funke, *Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht*, Baden-Baden, 2017, p. 82 ss., e, in parte, anche G. von Zimmermann, *Die Einwilligung im Internet*, Berlin, 2014, p. 13 ss. (il quale sottolinea anche la congruità, rispetto agli interessi in gioco, della qualificazione nei termini di negozio).

46 Non mi sembra che, invece, aiuti a qualificare in un senso o nell'altro l'osservazione – pur corretta – secondo cui ogni inquadramento deve tenere a mente la fisiologica ammissibilità del trattamento dei dati, che non costituisce certo ipotesi eccezionale: e, ciò, sia perché tale considerazione non esclude la qualificazione come autorizzazione (seppur di tipo diverso dal consenso dell'avente diritto: cfr. F. Bravo, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e Impresa*, 2019, p. 42), sia perché a valle si ripropone il problema – assai arduo e acuito dalla prospettiva eurounitaria – della qualificazione dell'autorizzazione (cfr. G. Oppo, *«Trattamento» dei dati personali e consenso dell'interessato*, in, *Scritti giuridici*, VI, *Principi e problemi del diritto privato*, Padova, 2000, p. 112).

sono avvertiti come centri di interessi (autonomi e distinti rispetto agli interessi che si situano a valle rispetto al loro trattamento). La qualificazione giuridica, anche degli atti di autonomia, si basa sulla realtà socio-giuridica, ossia sul modo di intendere i valori in gioco in seno alla società (per come esso si proietta sull'ordinamento e si definisce all'interno dell'ordinamento). Se, poi, la percezione generale si discostasse dalla stessa realtà socio-giuridica, non si potrebbe comunque negare che solo quest'ultima è la base su cui compiere la qualificazione giuridica, pur dovendosi rilevare uno scarto con la percezione generale[47].

La qualificazione del consenso come negozio impone, più precisamente, di rinvenirvi un atto di disposizione: un negozio unilaterale volto al trasferimento costitutivo di un diritto. Questo diritto, a sua volta, ha ad oggetto un bene – in senso atecnico – personale; il diritto, tuttavia, sfugge alla distinzione tra personalità e patrimonialità[48], finendo per innestarsi nella specifica libertà o nello specifico diritto cui di volta in volta è più legato (ora alla libertà di espressione, ora alla potestà pubblica e così via). Solo nel caso in cui tale libertà altro non è che quella economica, come nei casi in cui il trattamento dei dati serve per finalità di *marketing* o simili, potrebbe ipotizzarsi che il diritto assuma dal lato del titolare del trattamento un valore patrimoniale e, di riflesso, che così si connoti (almeno in parte) pure il suo oggetto: ciò

---

47 Questo scarto, tra il piano dei valori effettivamente immanenti alla società (in sé e per sé e per come la costruzione sociale si proietta e si definisce sul piano dell'ordinamento giuridico) e la stessa percezione che la società ha dei valori (che condivide e che proietta sul sistema giuridico), è tipico della protezione dei dati e deriva dal "paradosso della valutazione" di cui si è già detto: sicché al tempo stesso certi valori sono inevitabilmente propri di un certo sistema socio-giuridico, ma di ciò spesso non se ne ha una generale e piena contezza. Sulla difficoltà di applicare i concetti di volontà e consenso a fronte degli atti di disposizione dei dati personali v. anche G. RESTA e V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, p. 411 ss.

48 Considerazioni simili, pur declinate in modo diverso da quanto qui sostenuto e comunque con notevole varietà di accenti, sono diffuse nella dottrina italiana: di "duplicità di rilevanza giuridica" parla I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale*, in *Annali dell'Università degli Studi Suor Orsola Benincasa*, 2016-2018, p. 24 (richiamando il noto scritto di G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 256 ss.); a favore di un superamento della tradizionale separazione tra patrimonialità e non patrimonialità si esprime R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contratto e Impresa*, 2020, p. 760.

che, conseguentemente, imporrebbe di rinvenire nel negozio l'atto di disposizione di un bene (anche) patrimoniale.

Se tutto questo è vero, non può però nemmeno sottacersi che, a questo livello assai generale la qualificazione dogmatica non appare di alcuna utilità, giacché, da un lato, risulta assai difficile creare a livello interpretativo una disciplina generale del negozio eurounitaria e, da un altro lato, essa risulterebbe praticamente del tutto superata e disattivata da quella prevista dal GDPR per l'atto di consenso.

6.5.2. I riflessi specifici

Probabilmente, scendendo più nel dettaglio potrebbe in qualche modo recuperarsi una qualche precettività – una qualche utilità pratica e deontologica – anche per l'inquadramento dogmatico. Sennonché, altri problemi finirebbero per emergere: da un lato, questi tratti specifici di disciplina risulterebbero ancora meno attingibili in via di interpretazione del diritto eurounitario di quanto non avvenga per il generico inquadramento del consenso nella categoria del negozio (e ciò sarebbe vero, anche se ci si basasse unicamente sulle tradizioni nazionali e sugli strumenti di *soft law*); da un altro lato, a ben vedere anche tali tratti di disciplina mancherebbero di un'effettiva precettività, perché di fatto sarebbero legati a profili non di particolare rilievo o comunque assorbiti dalla disciplina prevista dal GDPR per l'atto di consenso.

Vediamo, a titolo di esempio, tre profili che appaiono di interesse. Premetto sin d'ora che escluderò dall'ambito dell'indagine ogni profilo inerente ai vizi del consenso, che appaiono strumenti inidonei a risolvere i nostri problemi, sia per il loro funzionamento operativo, sia per la loro connessione con situazioni di patologia (mentre, come si è visto, il punto dolente del consenso al trattamento deriva dalla fisiologica assenza di una volontà reale e realmente ponderata).

Anzitutto, va ricordato che in numerosi ordinamenti europei i contratti che non sono sostenuti da uno scambio o quanto meno da un interesse patrimoniale del disponente (secondo il lessico italiano) debbano venire ricondotti alla donazione, la quale sarebbe soggetta a un particolare onere di forma (solo in alcuni sistemi superabile in virtù dell'esecuzione del contratto). Ci si potrebbe allora chiedere se, quando il dato assurge a bene patrimoniale, la disposizione dello

stesso debba avvenire per forza di cose a titolo di scambio (anche solo empirico o interno), onde evitare la qualificazione di donazione.

Un simile esito, pur apparentemente controintuitivo, in realtà potrebbe apparire opportuno da un punto di vista di disciplina. In tal modo, infatti, non si escluderebbe che la disposizione del bene personale sia e resti un atto dominato da profili personali[49]; semplicemente, si introdurrebbe una ulteriore qualificazione, tale da richiedere, al fine di rendere valida la disposizione, di rinvenire uno scambio (come detto, anche solo empirico o interno)[50]. Ove così non fosse, la disposizione sarebbe nulla – perché priva della forma donativa – e, parimenti, il consenso non sarebbe validamente prestato, con tutto ciò che ne consegue. Il dibattito, ormai assai noto, circa l'ammissibilità che i dati divengano *consideration* dovrebbe allora risolversi nel senso che, ogni qual volta i dati costituiscono anche beni patrimoniali, il negozio – in tal caso presumibilmente un contratto – non solo può, ma addirittura deve prevedere una controprestazione o comunque un interesse patrimoniale in capo al disponente, soddisfatto mediante la stessa disposizione.

Nei fatti, però, questa conclusione non è persuasiva. Da un lato, così come è difficile applicare il diritto interno al negozio di consenso, così

---

[49] Nel caso di concessione del diritto di sfruttare economicamente l'immagine il contesto patrimoniale supera, in qualche parte, quello personale, che pur continua a deformare la disciplina del contratto (dal lato del disponente). Nel caso di dati personali, invece, le due dimensioni rimangono per forza di cose indipendenti e contemporaneamente esistenti, poiché la dimensione patrimoniale non rende in alcun modo meno pressante l'esigenza di tutela legata alla personalità del bene: prova ne sia che, per il GDPR, in tutti i casi il consenso è sempre revocabile (senza che l'affidamento di controparte abbia mai un ruolo, diversamente da quanto sosteneva la dottrina nel vigore della precedente Direttiva: cfr. S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, I, Milano, 2006, p. 1053 s.); e ulteriore conferma si può trarre dal fatto che, in questi casi, la patrimonialità non diminuisce le note legate all'esigenza di protezione dell'individuo (come invece può avvenire in tutti i casi in cui l'immagine viene "venduta"). Più in generale, a proposito del fatto che "il richiamo all'idea di mercato" non "potrebbero essere inteso come indebolimento del grado di tutela rispetto al trattamento dei dati personali", cfr. V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Contratto e Impresa*, 2018, p. 1117.

[50] Di conseguenza, nell'atto dovrebbe rinvenirsi anche un solo contratto, e non già – come da taluno proposto – il collegamento tra due atti o un atto complesso (rispettivamente G. DE CRISTOFARO, *Die datenschutzrechtliche Einwilligung*, cit., p. 169 ss.; R. SENIGAGLIA, *Minore età e contratto. Contributo alla teoria della capacità*, Torino, 2020, in corso di pubblicazione).

è arduo ritenere che il diritto eurounitario si allarghi sino a disciplinare profili ulteriori e che da questi faccia discendere delle conseguenze di disciplina per lo stesso consenso[51]. Da un altro lato, da un punto di vista pratico il profilo non appare di grande importanza: non è difficile accorgersi che la disposizione di dati personali, in campo patrimoniale, può di regola essere fatta afferire all'interesse del disponente di ricevere una pubblicità targettizzata.

In secondo luogo ci si può domandare se, in virtù del moto di tutto il diritto privato contrattuale europeo verso una pregnante funzionalizzazione e un forte solidarismo, l'inquadramento non possa condurre a perimetrare l'ambito di validità del consenso al trattamento[52].

Una tale materializzazione potrebbe indurre a normalizzare fortemente l'interesse di cui ipoteticamente, e ragionevolmente, è portatore

---

51 Di conseguenza, appare preferibile ritenere di trovarsi di fronte a un negozio di consenso, collegato a un contratto e inserito in uno schema di sinallagma condizionale (v. Ph. Hacker, *Daten als Gegenleistung. Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht*, in *die Zeitschrift für die gesamte Privatrechtswissenschaft*, 2019, p. 148 ss.; sul sinallagma condizionale in Italia v. per tutti G. Amadio, *Controllo sull'esecuzione ed efficacia negoziale (note intorno al concetto di onere)*, in *Letture sull'autonomia privata*, Padova, 2005, p. 220 ss.; in senso contrario, ossia ipotizzando l'esistenza di un'obbligazione di fornire i dati, si esprime A. Metzger, *Dienst gegen Daten: Ein synallagmatischer Vertrag*, in *Archiv für die civilistische Praxis*, 2016, p. 833 ss.). Venuto meno il consenso, cadrebbe quindi il rapporto contrattuale (ma non viceversa, per quanto patologie del contratto o del rapporto possano essere valutate per verificare la validità dell'atto di consenso o l'eventualità di una revoca); né questo potrebbe rappresentare un pregiudizio illegittimo per il *data subject*, giacché un simile *detriment* corrisponderebbe in tutto e per tutto al vantaggio – giocoforza legittimo – ottenuto dallo stesso *data subject* concedendo il suo consenso (ritiene invece che la revoca del consenso non faccia venire meno il contratto principale, ma consenta alla controparte di recedere, G. De Cristofaro, *Die datenschutzrechtliche Einwilligung*, cit., p. 169 ss., il quale in tal modo si propone di evitare la scure del principio per cui la revoca del consenso non può comportare un pregiudizio per il titolare dei dati).

52 Sulla diffusa "materializzazione" del diritto privato europeo (inteso, qui, come diritto privato dei singoli stati europei, anche esterni all'Unione), v. C.-W. Canaris, *Wandlungen des Schuldvertragsrechts - Tendenzen zu seiner „Materialisierung"*, in *Archiv für die civilistische Praxis*, 2000, p. 273 ss.; A. di Majo, *Giustizia e "materializzazione" nel diritto delle obbligazioni e dei contratti tra (regole di) fattispecie e (regole di) procedura*, in *Eur. dir. priv.*, 2013, p. 797 ss.; Cass. com., 22 octobre 1996, in Bull. civ., IV, n. 261, e il conseguente art. 1170 Code civil, per come modificato dall'ampia riforma del 2016. Un simile moto è rilevabile – e già da tempi – finanche nel *common law* inglese, pregno di formalismo: v. la *red hand rule* di J Spurling Ltd v Bradshaw [1956] EWCA 3, poi applicata nel più recente Interfoto Picture Library Ltd v Stiletto Visual Programmes Ltd [1987] EWCA Civ 6.

il *data subject*, valutando in relazione a esso la validità dell'atto di consenso. Si potrebbe, in particolare, ritenere che, là dove un negozio di consenso ingloba un interesse opposto a quello ragionevole, esso è nullo o comunque invalido[53].

Tuttavia, a parte gli evidenti problemi di ricostruire un'effettiva disciplina eurounitaria di questo stampo, comunque non si potrebbe esasperare questo controllo, poiché altrimenti si negherebbe la stessa scelta autonoma del *data subject* e si finirebbe per far ridondare la base del "consenso" in quella del "legittimo interesse" (svuotando del tutto la prima[54]).

Di fatto, questa via, pur in qualche modo percorribile, finirebbe per permettere un sindacato sull'*an* solo in casi estremi e, per il resto, un sindacato sul *quomodo*: il quale, però, riguarderebbe ipotesi abbastanza limitate. Si pensi, ad esempio, al caso in cui un soggetto chieda a una società che gestisce un sito di intermediazione immobiliare di venire contattato da eventuali venditori per avere informazioni circa l'acquisto di un bene. Ora, a ben vedere, tale acquisto corrisponde a un interesse normalmente e fisiologicamente limitato nel tempo: sì che estendere eccessivamente l'ambito del consenso valido (ad esempio, ipotizzando che esso possa giustificare anche un trattamento senza durata temporale) parrebbe un'operazione illegittima proprio per il contrasto tra l'interesse normale del *data subject* e quello irragionevole che altrimenti sarebbe introiettato nell'atto di consenso.

Solo entro questi risicati limiti l'inquadramento eurounitario, unitamente a una forte solidarizzazione dell'autonomia privata, potrebbe risultare di una qualche utilità. E, a dire il vero, perfino entro questo perimetro esso, a ben vedere, non apporta nulla di nuovo: già oggi un'interpretazione fedelmente orientata ai principi di correttezza e di minimizzazione, insiti nel GDPR, dovrebbe consentire di giungere a risultati corrispondenti. Sì che, ancora una volta, sembra che la qualificazione dell'atto di consenso non sia di alcuna utilità.

---

53 Clausole generali e categorie analoghe alla "meritevolezza" di cui all'art. 1322, comma 2, c.c. verrebbe così piegate a sindacare l'effettiva presenza di un interesse conforme a quello di cui è ipoteticamente portatore il *data subject* in quella situazione.

54 Di fatto, si assisterebbe a un bilanciamento secondo normalità e ragionevolezza, volto a svuotare anche la facoltà per il titolare dei dati di scegliere l'*an* (a questi sarebbe lasciata solo la scelta di negare il trattamento, ma non di consentirvi; di fatto, il diritto di autorizzarlo si tradurrebbe in una richiesta di *opt-out* anticipata).

Un terzo, e ultimo, profilo da considerare riguarda quell'inquadramento eurounitario che deriva non già dall'applicazione di principi derivanti dalle varie tradizioni nazionali e dagli strumenti di *soft law*, ma semmai dal resto della disciplina eurounitaria: e, in particolare, da quella in tema di contratto del consumo e di pratiche commerciali scorrette[55].

In effetti, questa via è stata già proposta in varie sedi: ci si è chiesti, ad esempio, se nella richiesta di consenso si può rinvenire un contratto del consumo e, quindi, vi si può applicare il controllo legale e giudiziale sulle clausole vessatorie[56]. La risposta più persuasiva, tuttavia, è stata negativa, anzitutto perché, in effetti, è difficile che un atto di consenso presenti uno squilibrio tra diritti e obblighi[57].

Dal punto di vista, invece, delle pratiche commerciali scorretti, si è effettivamente ammesso che l'offerta di un servizio, indicato come "gratuito" là dove invece esso è prestato a fronte della corresponsione di dati, può costituire una pratica commerciale scorretta[58]. E, tuttavia, anche questo esito non sembra del tutto utile ai nostri fini, non solo perché intercetta un profilo assai specifico, ma anche e soprattutto perché il servizio in questione, indicato come gratuito e in realtà pagato tramite i dati, non richiede affatto un consenso per trattare questi dati,

---

55 V., in linea generale, G. De Cristofaro, *Die datenschutzrechtliche Einwilligung*, cit., p. 173 ss.

56 Interrogativo, peraltro, stimolato anche dal considerando 42 del GDPR, secondo il quale, in conformità alla Direttiva 93/13/CEE, la dichiarazione di consenso non dovrebbe contenere "clausole abusive".

57 Cfr. del resto l'art. 4, par. 2, Direttiva 93/13/CEE, secondo cui "la valutazione del carattere abusivo delle clausole non verte né sulla definizione dell'oggetto principale del contratto, né sulla perequazione tra il prezzo e la remunerazione, da un lato, e i servizi o i beni che devono essere forniti in cambio, dall'altro, purché tali clausole siano formulate in modo chiaro e comprensibile". In questo senso v. S. Thobani, *Processing Personal Data and the Role of Consent*, in *European Journal of Privacy Law & Technologies*, 2020, p. 100; cfr. anche Th. Pfeiffer, *Datenschutz und AGB-Recht: Die Inhaltskontrolle vorformulierter Einwilligungserklärungen*, in M. Weller e M. Wendland (hrsg.), *Digital Single Market. Bausteine eines Digitalen Binnenmarkts*, Tübingen, 2019, p. 60 ss.

58 V. da ultimo T.A.R. Lazio, Sez. I, 10 gennaio 2020, n. 260, in *Foro Amm. - TAR*, 2020, p. 99, a proposito della quale v. anche B. Parenzo, *Dati personali come "moneta". Note a margine della sentenza TAR Lazio n. 260/2020*, in *juscivile*, 2020, p. 1364 ss.

ma li processa sulla base dell'interesse legittimo (sì che, dal punto di vista italiano, il contratto appare piuttosto gratuito e atipico)[59].

A tal riguardo, l'intervento di un altro corpo normativo, ossia il diritto della concorrenza, potrebbe sortire un migliore effetto: a fronte, infatti, dell'impossibilità per l'utente di scegliere se accettare o meno pubblicità targettizzate, la giurisprudenza (questa volta, tedesca) ha affermato che, sebbene non costituisca un illecito (civile e amministrativo) in base alla disciplina del GDPR, la mancata richiesta di un consenso per il trattamento dei dati o comunque l'assenza di una scelta a tal riguardo può rappresentare un illecito anticoncorrenziale[60]. Tuttavia, anche questa prospettiva non ci aiuta a risolvere le disfunzioni del consenso in sé considerato: anzi, ampliandone il ruolo (e in un certo modo quindi invertendo il percorso intrapreso dalla regolamentazione della protezione dei dati personali), le rende ancora più preoccupanti.

La soluzione ai problemi già messi sul tavolo va cercata, evidentemente, altrove.

6.6. La disciplina: una seconda proposta (priva di appiglio normativo)

Escluso che la via dell'inquadramento dogmatico possa aiutarci a trovare le risposte che cerchiamo, non resta che chiedersi se, da un punto di vista funzionale, si possa immaginare di perimetrare in modo diverso e forse ancora più rigido il consenso al fine di renderne effettivo il sistema, al tempo stesso evitando di limitare eccessivamente la liceità del trattamento dei dati[61]. Vale la pena di porsi questa domanda prima in astratto, per poi verificare se un'eventuale risposta richieda un cambiamento di legislazione o semplicemente un adattamento della sua interpretazione.

---

59 V. l'informativa di Facebook all'url *https://www.facebook.com/about/privacy/legal_bases* (controllato per l'ultima volta il 30 novembre 2020). Qui la base del trattamento è costituita dal legittimo interesse perché, in effetti, non viene garantito un servizio a fronte della processabilità di un dato, che costituisce al tempo stesso la remunerazione del servizio (come avviene finanche nel caso di iscrizione a una *newsletter*); piuttosto, si offre un servizio a fronte di ulteriori utilizzi dei dati già validamente raccolti (utilizzi per lo più pubblicitari e comunque intrinseci allo stesso servizio che viene offerto).

60 Così, da ultimo, BGH, 23 giugno 2020 - KVR 69/19.

61 Sulla libera circolazione dei dati v. già l'art. 1 GDPR, oltre ai considerando 3 e 9.

6.6.1. Alla ricerca del consenso effettivo

Anzitutto, ogni riflessione dovrebbe ammettere che la disciplina del consenso non può essere identica per casi eccessivamente diversi. Ovviamente, ciò non potrebbe risolversi in un approccio atomistico al problema del consenso: tuttavia, bisognerebbe quanto meno riconoscere che talune ipotesi – e qui il riferimento va soprattutto al consenso ai *cookie* – sono assai diverse da altre.

E, difatti, il consenso ai *cookie* per sua natura è molto particolare: esso presenta, per di più, problemi di regolazione peculiari, dovuti alla natura della navigazione sul *web* (alla sua velocità e alla sua complessità tecnica[62]). Ritenere che il consenso ai *cookie* debba e possa venire disciplinato come ogni altro consenso vorrebbe dire rinunciare, in ogni situazione, all'effettività di questa base e della connessa dichiarazione negoziale. E un simile risultato, per quanto possibile, va scongiurato: anche, per l'appunto, distinguendo il consenso generale da quella sua sottospecie tipica che è il consenso ai *cookie*, che richiede una regolazione autonoma.

Prendiamo allora a riferimento la fattispecie generale e proviamo a indagare come, in questa sede, il consenso possa essere reso più effettivo (nella convinzione che, là dove sufficientemente effettivo, il consenso deve restare accessibile come base, sia perché è utile, sia per evitare un eccessivo paternalismo).

La direzione da intraprendere, in linea di massima, dovrebbe essere quella già percorsa dal legislatore eurounitario: quella, cioè, per cui il consenso è valido solo in presenza di una scelta che, in sé e per sé, riveli una normale attività decisionale e, quindi, un utilizzo normalmente idoneo e sufficiente delle proprie capacità cognitive (attenzione, concentrazione, ponderazione).

Alcuni esempi possono essere utili. Talune ipotesi sono abbastanza eclatanti: si pensi al caso in cui un soggetto chieda, in modo formalmente conforme al dettato del GDPR, il consenso a trattare i dati per una finalità inaspettata (una biblioteca chiede di pubblicare sul proprio sito *web* la fotografia personale contestualmente caricata dall'utente per ottenere una tessera di entrata). Il fatto che tale finalità sia anomala,

---

[62] Le quali rendono inevitabile, a tacer d'altro, la mancanza di una decisione analitica circa gli specifici scopi di trattamento dei *cookie*: il *data subject* di fatto accetterà tutto o, se e quando potrà farlo in blocco, rifiuterà tutto.

rispetto a quanto di norma avviene nel mercato o comunque nel settore di riferimento, induce a ritenere che la semplice spunta di una casella sia inidonea a rivelare il consenso. Una soluzione diversa potrebbe imporsi se, per fornire il consenso, l'utente dovesse cliccare su un apposito *link*, identificato dalla finalità in parola ("se vuoi che la tua immagine sia pubblicata, clicca qui"), e una volta reindirizzato dovesse decidere se accettare o meno il trattamento.

L'esito divisato potrebbe già ora imporsi sulla base di un'interpretazione funzionale del GDPR. Del resto, tutto il Regolamento è percorso dall'idea per cui più inaspettato è un trattamento, ossia meno usuale, normale e finanche necessario, più si ammorbidiscono i requisiti di liceità del trattamento (cfr., ad esempio, gli artt. 6, par. 4, e 9): il che, tradotto nei termini del consenso, parrebbe ammettere un livello di trasparenza e informazione minore, tutte le volte in cui il trattamento è di natura tale per cui l'interessato può aspettarsi che gli sia richiesto, in quella data situazione, il consenso per porlo in essere.

Altri esempi, invece, sono meno vistosi, ma comunque richiedono di venire (ri)considerati[63]. Si pensi, in generale, a tutte le *boxes*, anche non preselezionate, che appaiono durante la fase di conclusione di un contratto *online*: un utente che voglia assicurarsi un certo servizio potrebbe, in modo disattento, selezionarle tutte (magari supponendo che le ipotesi di consenso facoltative si riferiscano, come avviene per la prima, solo a una *newsletter*; oppure ipotizzando, nella rapidità della lettura, che si tratti in ogni caso di un consenso necessario per l'esecuzione del servizio). Allo stesso modo, nel caso di un *banner* pubblicitario di un sito internet che nasconde momentaneamente la pagina e chiede all'utente se voglia ricevere notifiche di aggiornamento, la presenza di un tasto "accetta" e di uno "rifiuta" non esclude che un soggetto sia portato ad acconsentire senza rendersi effettivamente conto – nella velocità della navigazione – della scelta chiamato a compiere (a maggior ragione se lo specifico oggetto, la provenienza e la frequenza delle notifiche fossero analiticamente specificate solo in una diversa pagina)[64]. La ragionevole certezza di un vero e proprio consenso richiederebbe, al contrario, di ottenere lo stesso consenso in modo ben

---

63 Si tratta di esempi in parte già citati al § 4.

64 Qualcosa di simile, ma legato alla particolare natura dei *cookie*, è previsto per i *cookie walls* nelle linee guida sul consenso dell'EDPB, su cui ci siamo soffermati nel § 3.

diverso: ad esempio, ospitando in pagine *web* recanti anche altri contenuti e diverse da quelle menzionate (e in particolare da quelle di conclusione di un contratto) spazi e *link* appositi, cliccando i quali il titolare dei dati possa *sua sponte* lasciare i suoi dati e acconsentire al trattamento stesso. In tal modo si eviterebbe un'eccessiva aggressività e si collegherebbe l'iniziativa volta a concedere il consenso a una scelta autonoma del *data subject*[65].

Ovviamente, si tratta di indicazioni specifiche, corrispondenti a principi generali da declinare a seconda delle specificità del caso: se la selezione dell'unica *box* oppure l'apposizione della firma per il consenso, anche in sede di conclusione del contratto, richiedesse al tempo stesso di inserire il proprio *account email* (non detenuto dal futuro titolare del trattamento), l'attenzione dell'interessato sarebbe attirata in modo maggiore e di ciò si dovrebbe inevitabilmente tenere conto[66]; parimenti, la richiesta di impostare il consenso in una *app* si abbina normalmente (proprio perché avviene *una tantum*) a un'attenzione maggiore dell'utente di quanto non accada con riferimento alle continue richieste che compaiono sulle pagine *web*.

E, ancora, in tutti i casi si dovrebbe presumibilmente indicare il trattamento non solo identificandone la finalità, ma anche rivelandone rischi e benefici e magari anche fornendone un'esemplificazione: questo, al primo livello in modo sufficientemente breve da non stancare il lettore (e da non indurlo a concedere il consenso senza aver finito di leggere) e, invece, in modo più analitico ai livelli ulteriori. Ad esempio, una società di sviluppo di *software*, nel chiedere il consenso a utilizzare

---

65 Il riferimento va soprattutto ad appositi spazi di pagine, come quelle di apertura, ove si preveda la possibilità di aprire altre pagine (ad esempio, di iscrizione a *newsletter*). In tal modo sarebbe assicurato un sufficiente livello di attenzione dell'interessato, che non capiterebbe di certo per caso sulla seconda pagina; e sarebbero evitate anche quelle richieste che, comparendo nell'ambito di pagine di transizione, spesso conducono a lasciare il proprio consenso solo e soltanto perché, nella rapidità del momento, non si ha il tempo per leggerle compiutamente e meno che meno per compiere una valutazione.

66 Anche la possibilità di scaricare una *app* a fronte del pagamento di un prezzo oppure gratuitamente, ma con necessità di prestare un consenso al trattamento, può rappresentare una modalità sufficientemente chiara per descrivere e far comprendere il "valore" dei dati che vengono ceduti (purché la *app* in questione non dia modo di usufruire di un servizio essenziale, nel qual caso il pagamento tramite dati comunque non sarebbe ammesso).

i dati relativi ad eventuali *crash* di una applicazione, dovrebbe evidenziare quali sono i rischi per il *data subject*, quali sono i benefici per il titolare del trattamento, quali sono i vantaggi per il *data subject* (normalmente, nessuno, se non genericamente quello di aiutare lo sviluppatore nella sua attività)[67]. Parimenti, la richiesta di consenso dovrebbe ben chiarire eventuali effetti collaterali: ad esempio, nel caso di pubblicazione di dati, il rischio – se esistente – di una futura impossibilità pratica e quindi inesigibilità giuridica per il primo titolare del trattamento di comunicare a tutti i terzi il venir meno sopravvenuto della base per il trattamento[68].

Ovviamente, più si volesse percorrere questa strada, più il consenso verrebbe limitato. Addirittura, in talune situazioni esso non sarebbe di fatto ammesso, proprio per l'impossibilità sostanziale di rispettare questi requisiti stringenti. Si tratta, però, di un esito che non è abnorme: già ora, in effetti, si ritiene inadatto il consenso in situazioni connotate da un rapporto asimmetrico tra le parti; per di più, il GDPR contiene numerose altre basi che, venendo debitamente estese[69], impedirebbero uno stallo e, per l'effetto, un'eccessiva compressione del principio di libera circolazione dei dati anche personali.

Anzi, rendere il consenso più effettivo può evitare che a esso ricorrano i titolari del trattamento di fatto per deresponsabilizzarsi, così non domandandosi – come invece sarebbe richiesto – se il singolo trattamento sia o meno autorizzato dalle altre basi del GDPR. Rendere il consenso "difficile", unitamente ad altri approdi ermeneutici cui è già

---

67 Anche qui, la previsione di un piccolo corrispettivo a favore di chi fornisce i suoi dati può costituire uno strumento idoneo a far comprendere che gli stessi dati hanno un "valore" instrinseco.

68 Cfr. art. 17, par. 2, GDPR.

69 Del resto, come si è detto, il legittimo interesse che preveda un *opt-out* non è altro che un consenso interamente materializzato. E, a tal riguardo, deve anche considerarsi che un *opt-out* di fatto si ha tutte le volte in cui le impostazioni di base di un apparecchio non consentano la raccolta di certi dati (ad esempio, quando si impedisce di *default* la raccolta di dati di geolocalizzazione alle *app* installate su uno *smartphone*). Peraltro, in tal caso deve ritenersi che la richiesta di ottenere i dati, giacché di fatto equivalente a un consenso, debba seguirne il più possibile il regime: se una *app* volta a memorizzare gli itinerari percorsi chiede di essere autorizzata ad accedere a quei dati, deve prima aver descritto la funzionalità in parola (così garantendo che l'utente sia attento) e poi, domandando il consenso, evidenziarne rischi e benefici, in forma sia sintetica che analitica (e sempre anche tramite esempi del trattamento).

in parte giunto l'EDPB – quello per cui, scopertasi l'inidoneità di una base, non la si può sostituire con un'altra a piacimento del titolare del trattamento[70] e quello per cui, chiesto e non ottenuto il consenso, non si potrebbe fondare il trattamento su un'altra base[71] –, vuol dire scongiurare questo risultato e superare questa prassi, oggi molto diffusa[72].

Al tempo stesso, un consenso reso più effettivo imporrebbe in numerose occasioni di ottenerlo non già formulando una di quelle richieste che, ai più, appare come una fastidiosa interruzione della navigazione: onde evitare che le circostanze risultino inidonee o che la richiesta al primo livello non risulti sufficientemente chiara e al tempo stesso breve, il potenziale titolare dovrebbe ottenere il consenso in altri modi[73]. Questo esito gioverebbe indirettamente anche ad altre finalità, permettendo di conseguire ulteriori risultati positivi che, di per sé, costituirebbero altrettanti argomenti a favore della revisione divisata.

In particolare, da un lato si eviterebbe il continuo disturbo recato dalle richieste di trattamento di dati (rispetto alle quali finanche il GDPR auspica che non interrompano continuamente la navigazione[74]); da un altro lato si stimolerebbe la creazione di una consapevolezza della concessione del consenso e, quindi, la formazione di una

---

70 § 123 delle menzionate linee guida sul consenso.

71 A tanto non arriva l'EDPB (e, peraltro, un tale esito non sarebbe probabilmente consentito dall'attuale testo del GDPR). Al contrario, le citate linee guida, al § 120, prevedono la possibilità per il titolare del trattamento di cambiare base (passando dal consenso a un'altra condizione di liceità), purché di ciò sia fornita l'informativa all'interessato ai sensi degli artt. 13 e 14 GDPR.

72 Peraltro, deve tenersi in considerazione anche l'ulteriore principio per cui non si può subordinare l'accesso a beni e servizi alla prestazione del consenso (in nessun caso, là dove beni e servizi sono essenziali; soltanto là dove sia preservata la libertà del consenso – ad esempio, consentendo di ottenere uno sconto tramite la concessione dei dati –, negli altri casi). Esso, a rigore, dovrebbe valere ed essere fatto valere anche là dove il consenso è necessario per l'adempimento di un'obbligazione, proprio perché nel momento in cui è chiesto il consenso non si dovrebbero far valere considerazioni che di per sé potrebbero fondare una diversa base.

73 Ad esempio: inserendo un *link* nella pagina di apertura, da cliccare per iscriversi a una *newsletter*. Il *link* dovrebbe poi rimandare a una pagina con una breve descrizione esemplificativa del trattamento e dei rischi e dei benefici per le parti.

74 Cfr. il considerando 32, su cui anche *infra*.

cultura dei dati e, in fondo, in quell'auspicato mutamento antropologico, che renda non solo conosciuti, ma anzitutto riconosciuti i valori insiti nella protezione dei dati personali[75].

6.6.2. Necessità di riforme legislative

La direzione che si è indicata richiederebbe di reinterpretare svariate disposizioni del GDPR: il che, oltre a costituire di per sé un'operazione difficile e forse nemmeno ammissibile[76], si scontra apertamente con il tenore testuale di alcune disposizioni che, pur non riguardando specificamente la disciplina generale del consenso, impediscono una revisione ermeneutica.

In effetti, di primo acchito potrebbe sembrare che il percorso indicato – volto a restringere alquanto l'ambito del consenso al trattamento – sia in qualche modo suggerito dallo stesso GDPR: sia perché, come si è visto, è la strada su cui si sta muovendo l'EDPB (e così pure la Corte di Giustizia), sia perché, com'è stato a suo tempo accennato, sussistono talune disposizioni su cui far leva per proseguire su questa strada.

Tra queste, vale la pena di considerare quella parte del considerando 32, in cui il legislatore eurounitario richiede che l'atto di consenso non disturbi immotivamente la navigazione: previsione che potrebbe essere letta non solo a garanzia del *free flow of data*, ma anche, al contrario, come restrizione del consenso legittimo, tutte le volte in cui esso venisse "richiesto" dal titolare del trattamento tramite una do-

---

75 In realtà, è possibile che la stessa cultura dei dati sia altrove più diffusa di quanto non avvenga in Italia; e che, oltretutto, sia maggiore l'attenzione che, a costo di impiegare più tempo e più concentrazione, l'utente medio pone allorché deve dare il suo consenso (e, qui, mi riferisco soprattutto a quanto avviene in Germania, dove effettivamente la consapevolezza e l'attenzione verso i dati sono assai alte). Tuttavia, l'esistenza stessa di differenze culturali tra gli Stati membri dev'essere una preoccupazione del legislatore eurounitario, che deve farsene carico e deve adattare la figura dell'utente medio, non potendo fare esclusivo riferimento a quanto avviene entro i confini di uno Stato (e della sua corrispondente società).

76 Quanto meno perché, rispetto al sistema su cui è intervenuto il GDPR, la scelta del legislatore europeo appare abbastanza nitida nel senso su cui oggi si è assestata l'interpretazione prevalente, di cui si è detto nel § 3. Ad oggi, quindi, non appaiono mature le condizioni per rendere ammissibile una nuova lettura delle disposizioni, che richiederebbe per lo meno una certa distanza temporale dalla scelta politica compiuta a livello legislativo.

manda che interrompe la navigazione (e che, quindi, richiede una risposta, anziché essere prodromica a una solo eventuale iniziativa dell'utente, volta a consentirgli di fornire spontaneamente i suoi dati personali)[77].

Quanto, poi, all'art. 7, par. 3, GDPR, il quale prevede che la revoca del consenso debba essere possibile con modalità tanto semplici quanto la concessione dello stesso, esso, a ben vedere, potrebbe anche venire letto *a contrario*: non solo, cioè, come volto a potenziare e facilitare la revoca, ma anche come diretto a limitare il consenso. Se la revoca richiede – e questo è inevitabile – un atto di iniziativa del *data subject*, così dovrebbe essere anche per il consenso, che, per realizzare l'accennata simmetria, dovrebbe presupporre un atto di iniziativa dello stesso *data subject*[78].

Tuttavia, per quanto convincenti siano queste argomentazioni, esse non appaiono del tutto persuasive; soprattutto, poi, resta innegabile che il GDPR ammette pacificamente talune modalità di ottenimento del consenso che, nella prospettiva in cui ci siamo posti, dovrebbero risultare inammissibili.

Si pensi, in particolare, all'enfasi con cui il GDPR richiama la "richiesta" al trattamento dei dati: la centralità che essa assume (ad esempio, al considerando 32 o all'art. 7, par. 2) lasciano trasparire che l'accettazione di una simile richiesta può costituire valido atto di consenso, benché in un sistema volto a rendere più effettivo il consenso essa dovrebbe essere considerata quasi sempre sarebbe insufficiente (proprio perché il consenso, per essere validamente prestato, dovrebbe abbinarsi a una scelta e soprattutto a una iniziativa in qualche misura spontanea del *data subject*).

E si pensi anche al consenso in ambito sanitario o legale, previsto dal sistema del Regolamento finanche dove i dati sensibili debbono essere trattati per finalità contrattuali (legate, cioè, all'adempimento di

---

77 In altri termini, se la richiesta di consenso non può interrompere la navigazione immotivamente, allora dovrebbero a rigore non essere ammesse richieste che colgono di sorpresa l'utente e in questo modo strappano un veloce consenso; proseguendo per questa via, la legittimità stessa di una richiesta – ossia di un atto la cui iniziativa proviene dal futuro titolare del trattamento – potrebbe venire posta in dubbio.

78 Ovviamente, non ci si riferisce a un'iniziativa del tutto spontanea, ma semmai incanalata dal titolare del trattamento, che potrebbe nelle sue pagine *web* indicare, in appositi spazi, la possibilità di conferire i propri dati personali per finalità specifiche (ad esempio, per l'iscrizione a una *newsletter* o per l'ottenimento di uno sconto).

un contratto). Qui davvero sarebbe difficile richiedere qualcosa in più di un semplice consenso a una richiesta altrui: sicché l'interpretazione che si è proposta risulterebbe inidonea a tenere in considerazione questi casi, per come attualmente regolati, finendo per risultare inattendibile e infondata in un'ottica *de iure condito*.

Ciò non toglie che, per mezzo di una riforma legislativa[79], si potrebbe rendere il consenso più effettivo: si tratta, del resto, di una strada che già il GDPR ha percorso, riconoscendo l'importanza di basi legali quali il legittimo interesse e irrigidendo i requisiti che il consenso deve presentare per essere valido; una strada che, però, non è ancora giunta alla metà, giacché il legislatore eurounitario ha, evidentemente, preferito accogliere soluzioni di compromesso.

Una futura revisione legislativa dovrebbe, in particolare, intervenire sulla disciplina generale del consenso, prevedendo – oltre a quanto già disposto – che il consenso non sia ammissibile quando, per le sue circostanze[80] o per il suo contenuto[81], l'attenzione che un soggetto normalmente vi dedicherebbe non è sufficiente a ritenerlo espressione di una volontà vera o veramente ponderata (ora perché l'attenzione è scarsa, ora perché, anche se profonda, non è di per sé tale da permettere una piena comprensione). Ciò che richiederebbe, ovviamente e come già ora accade, l'elaborazione di una tassonomia volta a riempire di significato questa indicazione generale.

Al tempo stesso, si dovrebbero conseguentemente ampliare le altre basi. Ciò che avverrebbe non solo in via interpretativa, ma anche legislativa: ad esempio, introducendo l'adempimento quale base anche

---

79 In quella che sarà la "sesta" generazione di regolazione della protezione dei dati. Sulle prime quattro generazioni cfr. V. MAYER-SCHÖNBERGER, *Generational Development of Data Protection in Europe*, in P.E. AGRE e M. ROTENBERG (eds), *Technology and Privacy: The New Landscape*, Cambridge (Massachusetts), p. 219 ss.; sulla quinta generazione v. N. KATZ, *Could GDPR Introduce The Fifth Generation Of Data Security?*, in *Informationsecuritybuzz*, 5 giugno 2018.

80 Ad esempio, in sede di conclusione di un contratto o comunque interrompendo la navigazione. Sarebbe ammesso invece chiedere di fornire il consenso all'interno di una pagina *web* con altri contenuti, prevedendo che l'utente che voglia – ad esempio – iscriversi a una *newsletter* debba cliccare su un *link* e, lì, sottoscriverla.

81 Ad esempio, perché eclatantemente disassato rispetto a quanto avviene in situazioni analoghe oppure perché ragionevolmente non frutto di una ponderazione sufficiente di rischi e benefici. Sarebbe permesso invece domandare il consenso se si spiegassero, in forma concisa e chiara, rischi e benefici, esemplificando il tipo di trattamento.

per il trattamento dei dati sensibili, tutt'al più previa ulteriore "conferma" dell'interessato[82]; oppure estendendo l'ambito in cui è possibile un *opt-out* del *data subject*[83].

Una riforma, peraltro, potrebbe e dovrebbe accompagnarsi a una separazione del consenso al trattamento dal più specifico consenso nel caso di *cookie*: il quale, come si è detto, ne rappresenta un ambito speciale, che non può fungere da modello, a pena di rendere sempre il consenso ineffettivo.

A sua volta, il consenso ai *cookie* richiede, per vedersi migliorato nella sua disciplina, un intervento che elimini quella strutturale e fisiologica asimmetria, per cui gli utenti, nel fornire il consenso, non hanno a disposizione che pochi secondi (al fine di non rendere eccessivamente lenta la navigazione in internet), a fronte di una moltitudine di *cookie* rispetto a cui compiere scelte specifiche. La soluzione, che tra l'altro consentirebbe di rendere meno "disturbante" la richiesta di consenso per i *cookie*, potrebbe passare attraverso l'agglutinazione di queste singole e specifiche scelte, da compiere *ex novo* per ogni sito, in un'unica decisione prodromica alla navigazione e differente a seconda di macro-categorie di *cookie*, differenziati per la finalità dello specifico trattamento; una decisione che avverrebbe modificando le impostazioni del *browser* (e, tutt'al più, consentendo all'utente di cambiarle per siti specifici[84]).

In un senso per lo meno simile si muoverà, presumibilmente, il legislatore europeo, che nel progetto di Regolamento *ePrivacy*[85], volto a

---

82 Essa rappresenterebbe, più che un atto di consenso, una sorta di "informativa rafforzata" (ovviamente, lo dico in senso atecnico, e nella consapevolezza che si richiederebbe un'attenta qualificazione dogmatica di questa "conferma"). Una simile "conferma" potrebbe essere regolata in modo analogo a quel particolarissimo "consenso" (che in realtà consenso non è) di cui si è parlato alla nt. 69.

83 Attualmente il legittimo interesse è ritenuto base sufficiente per il *soft spam*, ossia per la pubblicità proveniente da soggetti con cui è già in essere un rapporto contrattuale (e sempre salvo, comunque, l'*opt-out*). Cfr., per quanto riguarda l'ordinamento italiano, l'art. 130, comma 4, d.lgs. 196/2003.

84 Si pensi ai siti che vendono prodotti desiderati dall'utente, che vuole quindi ricevere una pubblicità targettizzata.

85 Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (Regolamento sulla vita privata e le comunicazioni elettroniche).

sostituire la Direttiva 2002/58/CE, ha previsto tra l'altro che "[i] programmi immessi sul mercato che consentono le comunicazioni elettroniche, compreso il recupero e la presentazione di informazioni in rete, offrono l'opzione di impedire che terzi conservino informazioni sull'apparecchiatura terminale di un utente finale o trattino le informazioni già conservate su detta apparecchiatura. All'installazione il programma informa l'utente finale delle impostazioni relative alla vita privata e per proseguire nell'installazione richiede il consenso dell'utente per una data impostazione" (così all'art. 10[86]).

Resta poi l'esigenza, che in altra sede si era già rilevata[87], di non chiedere alla disciplina della protezione dei dati troppo o comunque qualcosa che essa non può dare. Probabilmente il consenso ai dati dovrà restare per sempre quale base; nondimeno, anche se particolarmente ristretto, esso finirà per nascondere in sé per sempre delle disfunzioni che lo allontano dal modello volontaristico contrattuale, rendendolo in buona parte ineffettivo.

Ciò non toglie, però, che per lo meno i riflessi negativi del consenso concesso potrebbero essere, se non eliminati, per lo meno ridotti per mezzo di una disciplina volta a ristabilire i diritti e gli interessi del titolare dei dati, di per sé compressi dallo stesso trattamento. E, infatti, se è vero che di regola il consenso al trattamento riguarda finalità in senso lato pubblicitarie, connesse al *direct marketing*, giocoforza è anche vero che una disciplina dello stesso *direct marketing* potrebbe restituire al *data subject* quella libertà di autodeterminazione commerciale che un consenso poco ponderato comprime (e, soprattutto, comprime senza che vi sia stata una scelta reale dello stesso *data subject*)[88].

Tutto questo, peraltro, assume importanza anche da un altro punto di vista. Il consenso al trattamento, anche se mai fosse totalmente effettivo, rischia di risultare distruttivo rispetto al sistema del GDPR an-

---

[86] Ma a tal riguardo v. anche il considerando 32 del GDPR, ove menziona – quale strumento per dare il consenso – "la scelta di impostazioni tecniche per servizi della società dell'informazione". Tale previsione, oggi, rischia di condurre a risultati assurdi (basterebbe non navigare "in privato" per acconsentire a tutti i *cookie*): sicché proprio il suo completamento nel Regolamento *ePrivacy* appare vieppiù necessario.

[87] Cfr. A.M. GAROFALO, *Protection*, cit.

[88] Ad esempio, si potrebbe prevedere – a livello di diritto del consumo – che le pubblicità profilate debbano dichiarare di esserlo e che, tramite una richiesta specifica, l'utente possa venire a conoscere i dati da cui deriva la sua profilazione.

che in un ulteriore senso, su cui finora non mi sono soffermato: la protezione dei dati ha un riflesso non solo individuale, ma anche – e forse soprattutto – sociale. Problemi come quello della *filter bubble* pongono pericoli, soprattutto per la tenuta sociale (e finanche istituzionale), che superano sicuramente la dimensione del singolo; problemi rispetto a cui un atto di consenso pone ovviamente dei rischi (quanto meno di *free riding*), che sicuramente non sono evitati solo perché il consenso è più effettivo e che, invece, richiedono di intervenire a valle, restituendo ai singoli quella capacità di giudizio altrimenti compromessa[89].

Insomma: se il consenso al trattamento resta irregolabile, ossia difficile o impossibile da regolare, forse è necessario spostare l'attenzione e disciplinare altri aspetti legati alla compressione degli interessi e dei diritti del singolo: altri aspetti, cioè, di un fenomeno che in fin dei conti da un punto di vista sostanziale rimane unitario.

[89] Ad esempio, inserendo una quota minima e necessaria di pubblicità e di notizie o opinioni giornalistiche non profilata, affinché nella libertà del caso si recuperi anche la libertà dei singoli v. S. Rodotà, Privacy *e costruzione della sfera privata*, in *Tecnologie e diritti*, Bologna, 1995, p. 121.

Il volume contiene contributi di docenti e ricercatori di varie Università italiane su una pluralità di tematiche che sollecitano la riflessione circa la tenuta delle categorie tradizionali del diritto privato a cospetto delle trasformazioni dei modelli di relazione tra i privati recate dalle tecnologie digitali. Gli scritti sono maturati nel contesto delle attività di ricerca e seminariali promosse dall'Osservatorio Giuridico sulla Innovazione Digitale (OGID), costituito presso il Dipartimento di Diritto ed economia delle attività produttive dell'Università Sapienza di Roma.

I curatori dell'opera, **Salvatore Orlando** e **Giuseppina Capaldo**, sono professori ordinari di diritto privato presso il Dipartimento di Diritto ed economia delle attività produttive di Sapienza Università di Roma.

ISBN 978-88-9377-186-3

www.editricesapienza.it