GIURISPRUDENZA E AUTORITÀ INDIPENDENTI NELL'EPOCA DEL DIRITTO LIQUIDO

STUDI IN ONORE DI ROBERTO PARDOLESI

A cura di F. Di Ciommo e O. Troiano

ISBN: 9788893179799

IL FORO ITALIANO

FONDATO NELL'ANNO 1876 DA ENRICO SCIALOJA

LaTribuna

Questo volume è pubblicato con la sponsorizzazione
dello Studio Legale Di Ciommo & Partners
e di IP2Tech S.r.l. – Industria Partecipazioni Tecnologia

La Tribuna Srl | www.latribuna.it
29121 Piacenza – Via Campo della Fiera, 4
Tel. 0523.46311 – Fax 0523.757219

Collisioni transatlantiche: consenso e contratto nel trattamento dei dati personali

di Michele Graziadei

Sommario: 1. Introduzione. – 2. Gli amici americani, e noi europei: due o tre differenze salienti in materia di protezione dei dati personali. – 3. Un quadro normativo frammentato e un consenso 'debole'. – 4. Il consenso e la cornice dei requisiti inderogabili che lo circondano. – 5. Terreni comuni.

1. Introduzione.

La rapida evoluzione delle tecnologie digitali e la loro diffusione su scala mondiale ridisegna ormai la vita della popolazione dell'intero pianeta. Al tempo stesso, la loro regolazione mette a nudo tensioni di fondo tra le varie aree del globo. Così, la regolazione del trattamento e del flusso dei dati tra Europa e Stati Uniti è attraversata da tensioni che non sono destinate a essere sopite a breve, né hanno carattere episodico, riflettendo tratti significativi di ciascuna esperienza a confronto. Ricordiamo a questo proposito - per il suo valore sintomatico - la recente risoluzione del Parlamento europeo che stigmatizza il livello inadeguato di protezione dei dati personali concretamente offerto dallo scudo UE-USA per la privacy (*privacy shield*)[1]. Con questo atto il Parlamento Europeo invita la Commissione Europea a sospendere l'accordo in questione per assicurare il rispetto integrale da parte delle autorità statunitensi delle condizioni stabilite per poter ritenere legittimo il flusso transfrontaliero dei dati verso l'altra sponde dell'Atlantico alla stregua del Regolamento (UE) 2016/679. La risoluzione del Parlamento Europeo ripercorre i nodi principali del discorso, ed è chiaro che non si tratta di questioni di poco conto, essendo in gioco la tutela di diritti fondamentali. D'altra parte, le cronache espongono in prima pagina con cadenza ormai quasi quotidiana horror stories transatlantiche relative alla violazione di dati personali, che non possono essere archiviate come meri incidenti di percorso, valga per tutte la violazione di cui Facebook è chiamato a rispondere nel caso Cambridge Analytics. In effetti, la risoluzione del Parlamento europeo sopra ricordata è solo una delle linee di attacco al tema in Europa. È infatti pendente davanti alla Corte di giustizia la questione preliminare sollevata dall'Alta Corte irlandese nel cosiddetto caso Schrems II, che investe a sua volta la legittimità del *Privacy Shield*[2]. L'accordo tra l'Unione

(1) Risoluzione del Parlamento europeo sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy (2018/2645(RSP)). La decisione della Commissione europea del 12 luglio 2016 n. 2016/1250 (in GU L 207 del 1.8.2016, pagg. 1–112), che è passata alle cronache come "scudo per la privacy", è stata ripresa da un provvedimento del Garante per la privacy italiano: Autorizzazione al trasferimento di dati all'estero tramite l'accordo denominato "EU-U.S. Privacy Shield - 27 ottobre 2016 (Pubblicato sulla Gazzetta Ufficiale n. 273 del 22 novembre 2016).

(2) Le questioni preliminari sottoposte dall'Alta Corte irlandese alla Corte di giustizia sono state formulate lo scorso 14 aprile 2018. La richiesta di Facebook di una sospensiva quanto all'invio degli atti alla Corte è stata respinta dal giudice irlandese. Tutti

europea e gli Stati Uniti che ha preso questo nome, com'è noto, ha sostituito il precedente *safe harbour agreement* nel regolare il flusso transfrontaliero dei dati tra l'Europa e gli Stati Uniti. Quest'ultimo era caduto nel 2015 sotto i colpi delle censure formulate dalla Corte di giustizia nella sentenza resa in Maximillian Schrems v. Data Protection Commissioner, con cui la Corte riteneva che il *safe harbour agreeement* violasse gli art. 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea[3].

Non tutti i segnali che provengono dal fronte sono però dello stesso segno, non tutti ci parlano di collisioni transatlantiche in materia di protezione di dati personali. Sempre nel 2018, la California ha promulgato una legge sulla privacy che si avvicina nella sua filosofia di fondo al Regolamento europeo in materia di protezione dei dati personali[4]. Pur non avendo un approccio altrettanto comprensivo, la novità che in California è maturata sull'impulso di una proposta di referendum popolare è stata salutata come una svolta nella materia rispetto alle *privacy laws* accolte negli altri Stati della federazione[5]. E un *think tank* privato come il *Council for foreign relations* ha espresso a sua volta opinioni favorevoli alla riforma del diritto statunitense nella medesima direzione. Si tratterebbe di sviluppare un approccio più comprensivo e integrato al tema della protezione dei dati personali, maggiormente allineato allo standard europeo, per superare la frammentazione che caratterizza il diritto statunitense in materia, e ne determina la scarsa influenza sul piano internazionale[6]. Il livello di fiducia manifestato dai cittadini statunitensi nei confronti del regime di protezione dei dati personali cui sono soggetti è d'altra parte effettivamente piuttosto basso[7]. Ma più in generale, non è detto che le aspettative dei cittadini statunitensi in materia di trattamento dati siano completamente diverse da quelle maturate in Europa. Indagini empiriche condotte sul punto mettono in luce significative e inaspettate convergenze al riguardo[8]. Nel frattempo, l'approvazione nel 2018 da parte dell'amministrazione Trump del CLOUD Act, destinato a regolare gli effetti di mandati statunitensi rivolti ad ottenere dati su server collocati all'estero, ma sotto il controllo di imprese americane, e l'accesso a informazioni su server localizzati nei USA da parte di autorità giudiziarie straniere, mette in luce come la sensibilissima materia del trattamento e del flusso di dati non sia certo considerata di secondo piano da parte dell'amministrazione statunitense[9].

Roberto Pardolesi ha esplorato con impareggiabile sagacia e spirito precorritore un ampio ventaglio di temi a cavallo tra l'economia e il diritto. Nelle sue brillanti ricerche, cui siamo tutti debitori, è costante l'attenzione dedicata all'impatto di tecnologie emergenti sul diritto in prospettiva transatlantica. Questo saggio riprende la medesima prospettiva, nella forma più modesta dei 'primi appunti', e

---

gli atti relativi alla lite, compresa la sentenza resa dall'Alta Corte irlandese il 17 Ottobre 2017, con cui il giudice ha deciso di formulare le questioni preliminari nel caso in questione, sono pubblicati sul sito della Data Protection Commission irlandese https://dataprotection.ie/.

(3) Causa C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650; su questa sentenza si vedano i contributi raccolti in: G. Resta, V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, RomaTrE-Press, Roma 2016.

(4) California Consumer Privacy Act 2018.

(5) Per la rassegna di queste leggi si consulta utilmente: National Conference of State Legislatures, State Laws Relating to Internet Privacy, <http://www.ncsl.org/> (ultimo accesso 13 luglio 2018).

(6) N. O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, <https://www.cfr.org/report/reforming-us-approach-data-protection> (consultato il 13 luglio 2018).

(7) Pew Research Center, *Americans and Cybersecurity* (January, 2017), <http://www.pewresearch.org> (consultato il 13 luglio 2018).

(8) J. Turow, *Americans and Marketplace Privacy: Seven Annenberg National Surveys in Perspective*, in E. Selinger, J. Polonetsky, O. Tene (a cura di), *The Cambridge Handbook of Consumer Privacy*, Cambridge U.P., Cambridge, 2018, p. 150, p. 165, secondo cui: "to the claim that a majority of Americans consent to discounts because the commercial benefits are worth the costs, we find a new explanation: a large pool of Americans feel resigned to the inevitability of surveillance and the power of marketers to harvest their data. When they shop it merely appears they are interested in trade-offs.". In breve: "for most the explanation for giving up the data is resignation. They see no opportunity to get what they really want from digital marketers – the ability to control what the marketers know about them. In that context, their unpredictable responses to the blandishment of discounts reflects futility rather than rational trade-off strategies." (a p. 167).

(9) Clarifying Lawful Overseas Use of Data (CLOUD) Act, H.R. 1625, 115th Cong. div. V (2018). Questa legge federale ha sollevato la Corte Suprema dal compito di decidere la lite in United States v. Microsoft Corp. (Microsoft Ireland), No. 17-2, slip op., 3 (17 Aprile 2018) (per curiam). Per un primo commento: J. Daskal, *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, 71 Stan. L. Rev. Online 9 (2018)

tratta quindi brevemente, per cenni essenziali, alcuni temi legati alla regolazione del trattamento dei dati personali in una visuale comparata. Si intendono ripercorrere in primo luogo le ragioni immediate delle differenze di approccio che prevalgono nelle due aree. L'attenzione cadrà poi su aspetti più specifici del discorso, per segnalare, oltre alle divergenze, alcune convergenze che potrebbero essere fruttuosamente esplorate nel riflettere ulteriormente sull'esperienza maturata al riguardo sull'una e sull'altra sponda dell'Atlantico.

2. GLI AMICI AMERICANI, E NOI EUROPEI: DUE O TRE DIFFERENZE SALIENTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI.

Tra Europa e Stati Uniti vi sono differenze cospicue in materia di raccolta e di trattamento dati. Alcune di queste differenze sono molto note, ma meritano comunque di essere ricordate[10]. Il diritto europeo in questa materia si è sviluppato avendo acquisito come pietra angolare del discorso l'esistenza di un diritto 'costituzionale' alla protezione dei dati personali. Le costituzioni di alcuni paesi europei, redatte più recentemente rispetto a quelle risalgono al secondo dopoguerra, sono esplicite sul punto. Là dove manca il riferimento testuale nel documento costituzionale, la giurisprudenza ha elaborato la nozione, e le ha assicurato copertura costituzionale[11]. In ogni caso, nel quadro europeo, tanto la Convenzione europea dei diritti dell'uomo, quanto, in modo esplicito, la Carta dei diritti fondamentali dell'Unione europea, artt. 7 e 8, riconoscono come diritto fondamentale il diritto alla privacy e alla protezione dei dati personali. Questo diritto può essere oggetto di bilanciamento, come altri diritti fondamentali, tuttavia il nesso tra il diritto in questione e il concetto di dignità della persona ne assicura il rango primario in sede di giudizio di proporzionalità, nel caso di conflitto con altri diritti, in particolare con diritti di carattere economico, ma anche, ed in modo più controverso, rispetto al diritto all'informazione. Negli Stati Uniti, non troviamo indicazioni altrettanto univoche. La Costituzione federale offre limitati spunti in questo senso, come attestano il IV e il XIV emendamento. La giurisprudenza della Corte Suprema si è sua volta dimostrata restia ad elaborare un principio costituzionale equivalente a quello che in Europa garantisce la protezione dei dati personali, anche perché la giurisprudenza sul primo emendamento offre un'ampia copertura al trattamento dati senza il consenso dell'interessato[12]. Così, negli Stati Uniti, il trattamento dei dati personali da parte dei privati è libero, salvo eccezioni stabilite per legge. Le leggi in materia sono cresciute nel corso del tempo, ma non sono molto numerose, e hanno comunque tutte carattere settoriale, e non omnicomprensivo. Solo governo federale e le agenzie federali sono sottoposti ad un regime di più ampio respiro che è consegnato al Privacy Act del 1974, di cui peraltro sono noti numerosi limiti[13].

Ecco dunque la possibilità di presentare l'approccio prevalente negli Stati Uniti e in Europa come l'espressione di due mondi alternativi[14]: l'Europa avrebbe abbracciato un esteso 'rights talk', vale a

(10) P. M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 Harvard Law Review 1966 (2013); F. Bignami, G. Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 Law & Contemp. Problems 101 (2015); P.M. Schwartz, K. N. Peifer, *Transatlantic Data Privacy Law*, 106 Georgetown Law Jo. 115 (2017).

(11) Emblematica la vicenda tedesca su cui, in prospettiva comparata, Bignami e Resta, *Transatlantic Privacy Regulation*, cit.

(12) Vedi la discussione della giurisprudenza costituzionale in materia di privacy in D.J. Solove, P.M. Schwartz, *Information Privacy Law*, Wolters Kluwer, New York, 2017,

(13) Sul punto F. Bignami, *The Us Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens. Study for the LIBE Committee of the European Parliament*, 2015; GWU Law School Public Law Research Paper No. 2015-54.

(14) Per quanto segue vedi soprattutto P. M. Schwartz, K. N. Peifer, *Transatlantic Data Privacy Law*, cit.

dire: "a rights-focused legal discourse centered on the individual whose data is processed"[15]. Questo approccio europeo è alternativo all'approccio statunitense sotto diversi aspetti. Anzitutto, i principi costituzionali accolti in materia in Europa hanno efficacia orizzontale, vale a dire non vincolano unicamente il governo e gli apparati pubblici, ma si applicano anche nei rapporti tra cittadini ed imprese. Numerose ulteriori caratteristiche del modello europeo delineano altrettanti contrasti con l'esperienza statunitense, che viene ricondotta al paradigma del "marketplace discourse"[16]. Con quest'ultima etichetta si indica un modello di tutela che, salve specifiche norme di legge diversamente ispirate, è mirato sulle esigenze di protezione di un soggetto considerato come partecipante ad un mercato in cui i dati personali sono liberamente negoziabili. Non a caso, la Federal Trade Commission è l'agenzia federale maggiormente coinvolta nell'enforcement delle norme che salvaguardano la privacy[17], mentre in Europa il medesimo compito è affidato a organismi che devono godere le maggiori garanzie di indipendenza. Tra gli aspetti salienti del modello europeo, vi è la tendenza ad affermare il diritto fondamentale alla tutela dei dati personali come preminente. In Google Spain la Corte di giustizia nega che la tutela dei dati personali possa essere sacrificata in presenza del "semplice interesse economico del gestore di un siffatto motore di ricerca in questo trattamento di dati" (e fin qui - si potrebbe dire - nulla di nuovo), ma un simile approccio oscura indebitamente il diritto all'informazione, talché, secondo Roberto Pardolesi, le valutazioni in tal modo espresse dalla Corte di Lussemburgo sarebbero il preludio di un: "bilanciamento fortemente compromesso degli interessi in gioco"[18]. D'altra parte, la violazione delle norme poste a tutela dei dati personali in Europa è sanzionata indipendentemente dal fatto che essa porti con sé conseguenze di natura patrimoniale per colui che la subisce. Sotto tutti questi profili il diritto statunitense registra soluzioni di diverso segno rispetto al quadro europeo. E per tornare al punto da cui ha preso avvio il discorso, il diritto statunitense consente di trasferire liberamente i dati personali dei cittadini americani in paesi terzi, senza porre condizioni o vincoli al trasferimento, al fine di garantire un livello adeguato di protezione di tali dati all'estero.

(15) Ibid., p. 122.

(16) Così, Schwartz, Peifer, *Transatlantic Data Privacy Law*, cit. Attesta questo orientamento anche il rapporto sulla privacy preparato sotto la presidenza di Barak Obama: White House, *Consumer data privacy in a networked world* (2012), <*https:/ obamawhitehouse. archives.gov/sites/default/files/privacy-final.pdf*>. Il rapporto avrebbe dovuto spianare la strada ad una legge di riforma dell'intera materia che però non ha avuto seguito.

(17) C.J. Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, Cambridge U.P., Cambridge, 2016.

(18) Così R. Pardolesi, *L'ombra del tempo e (il diritto al)l'oblio*, Questione giustizia, 2017, § 2.2. (consultato nella versione online il 13 luglio 2018). Com'è noto, la sentenza della Corte da cui prende avvio il discorso è: C-131/12, Google Spain v. AEDP, in Foro italiano, 2014, IV, 295 con nota critica di R. Pardolesi e A Palmieri, *Diritto all'oblio: il futuro dietro le spalle*. Per ulteriori appunti critici su di essa: F. Di Ciommo, *Quello che il diritto non dice. Internet e oblio*, Danno e responsabilità, 2014, p. 1101 ss; O. Pollicino – M. Bassini, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburg* in G. Resta, V. Zeno Zencovich (a cura di) *La protezione transnazionale dei dati*, cit., p. 73 ff.. Gli sviluppi più recenti in proposito in sede europea sono commentati dal Pardolesi, *Oltre «Google Spain» e il diritto all'oblio*, nota a Consiglio di Stato della Repubblica Francese, assemblea del contenzioso; decisione, 24-02-2017, n. 391000, Foro it., 2017, IV, 219, in cui l'a. mette in luce il tema soggiacente alla pronuncia resa dalla Corte e la deriva argomentativa che traspare il tema non è più, propriamente, il diritto all'oblio, quanto piuttosto: "...[...] l'inibizione di attività illecite, perché chiaramente contrarie ad esplicite proibizioni normative. Per il gigante di Mountain Valley e i suoi emuli (Bing, Yahoo!, Yandex, Baidu e compagnia) si annunciano notti (europee) buie e tempestose.". La Corte di giustizia si è espressa in modo più prudente in relazione ai dati personali resi pubblici tramite il registro delle imprese: C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni, in Foro it., 2017, IV, 77, con nota di R. Pardolesi, *Non c'è diritto all'oblio per i dati personali nel registro delle imprese. O forse sì*. Nel frattempo, il diritto all'oblio si è insinuato ne Regolamento europeo 2016/679 sulla protezione dei dati personali. Le scelte realizzate dai redattori del nuovo testo hanno però a loro volta suscitato critiche: S. Bonavita, R. Pardolesi, *GDPR e diritto alla cancellazione (oblio)*, Danno e responsabilità, 2018 nr. 3. F. Di Ciommo, *Il diritto all'oblio (oblito) nel regolamento Ue 2016/679 sul trattamento dei dati personali*, Foro it., 2017, V, 306. Peraltro i giudici nazionali chiamati a decidere in concreto sul rilievo del diritto all'oblio del singolo ricorrente hanno frequentemente dato maggiore rilievo al diritto all'informazione. Così, la pretesa del ricorrente che ha dato origine a tutta la vicenda Google Spain è stata infine negata dalla Corte spagnola che ha reso la decisione sul punto, e come nota F. Di Ciommo, *Privacy in Europe After Regulation (EU) No 2016/679: What Will Remain of the Right to Be Forgotten?* Italian Law Journal, 2017, p. 623 ss., p. 644-645, la giurisprudenza italiana: "seeks to guarantee the utmost freedom of expression of those dedicated to informing the public".

Naturalmente, è possibile che queste differenze si attenuino in parte nella prassi dei maggiori operatori economici, come rivelano recenti indagini empiriche[19]. Tuttavia, è pur vero che le premesse del discorso, sotto il profilo dei riferimenti giuridici essenziali rimangono abbastanza distanti. Merita considerare a questo proposito il diverso approccio del diritto statunitense al consenso rispetto al trattamento dati e al ruolo che riveste il contratto come strumento per governare il trattamento dati oltre Atlantico.

3. Un quadro normativo frammentato e un consenso 'debole'.

Il diritto statunitense non richiede in via generale il consenso al trattamento dei dati come condizione per la liceità del trattamento. Vi sono tuttavia alcune leggi federali che dettano regole in materia di consenso rispetto al trattamento dati in ordine a determinate attività. Queste leggi talvolta stabiliscono il consenso come requisito per la liceità del trattamento, talvolta invece impediscono il trattamento qualora l'interessato vi si opponga negando il consenso al trattamento. In quest'ultimo caso, beninteso, il trattamento è lecito anche in difetto di consenso, purché non sia stata espressa opposizione da parte dell'interessato. Tuttavia, in ambedue i casi il rilievo del consenso è piuttosto limitato. Prevale in linea generale un approccio che, rispetto al quadro europeo, si può definire senz'altro più blando e meno ambizioso.

Il Fair Credit Reporting Act è il capostipite delle leggi federali che richiedono il consenso affinché il trattamento dei dati sia lecito[20]. La disciplina si applica all'uso dei dati relativi alla solvibilità dei consumatori che sono raccolti ed elaborati da imprese del settore. La legge ammette che queste informazioni siano diffuse e condivise liberamente per un vasto numero di finalità; l'impresa può, ad esempio, effettuare questa scelta semplicemente perché ritiene ragionevolmente che vi sia: "a legitimate business need for the information"[21]. Pertanto, di regola il trattamento dei dati personali relativi all'affidabilità creditizia del consumatore avviene senza il consenso di quest'ultimo. Prevale una diversa soluzione unicamente nel caso in cui le informazioni raccolte siano utilizzate dall'impresa in relazione a decisioni relative all'impiego del lavoratore, o in quanto si sia in presenza di dati che riguardano informazioni sulla salute dell'interessato. Un datore di lavoro, o un potenziale datore di lavoro, può quindi utilizzare questi dati solo dopo aver avvisato l'interessato in modo chiaro e evidente dell'uso che si intende fare di essi, e solo dopo aver ottenuto l'autorizzazione scritta dall'interessato. Le precauzioni sono rafforzate nel caso in cui l'informazione riferisca dati medici. Si noti però che questa disciplina ignora la possibilità di squilibri di potere. Essa non tiene conto del fatto che il lavoratore, che nega al datore di lavoro il consenso, avrà ben poche probabilità di veder confermata l'offerta di impiego.

In altri contesti, il consenso non è richiesto per la liceità del trattamento, ma è lasciata al consumatore la facoltà di opporsi al trattamento. Così in materia di condivisione dei dati all'interno dei conglomerati finanziari, secondo il Gramm–Leach–Bliley Act [22]. È stato notato che questa impostazione pone a carico del soggetto meno informato le conseguenze della mancata opposizione.

Più in generale, il diritto dei contratti negli Stati Uniti viene rapidamente messo fuori gioco come strumento di protezione dei dati personali. In effetti, le Corti hanno ripetutamente affermato che l'an-

(19) K. A. Bamberger, D. K. Mulligan, S. Braman, P. T. Jaeger (a cura di), *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*, M.I.T. Press, Boston, 2015.

(20) 15 U.S.C. § 1681 (2012)

(21) 15 U.S.C. § 1681b(a)(3)(F) (2012).

(22) 15 U.S.C. §§ 6801–6809 (2012).

nuncio da parte di una società determinata privacy policy applicabile ai clienti non è vincolante sul piano giuridico, in quanto non forma in realtà parte del contratto concluso con loro. Alternativamente, è stato deciso che la condivisione di dati personali in violazione di tale politica non è fonte di danni per le persone che la subiscono e quindi non può dar luogo a risarcimenti in loro favore.

4. Il consenso e la cornice dei requisiti inderogabili che lo circondano.

Le soluzioni brevemente illustrate nel paragrafo precedente sono in netto contrasto con le norme in materia di protezione dei dati personali che prevalgono in Europa, le quali hanno ricevuto statuto 'costituzionale' nella Carta dei diritti fondamentali dell'Unione Europea. Nell'Unione, il trattamento dati conforme a diritto non presuppone unicamente una delle basi legali enunciate ora nell'art. 6 del Reg. UE 2016/679, ma ancor prima richiede che, in presenza di tali presupposti, il trattamento dati rispetti comunque vari e stringenti requisiti ulteriori, richiamati nell'art. 5 del Regolamento, la cui violazione rende il trattamento senz'altro illecito.

L'Unione europea ha dunque stabilito una cornice di norme giuridiche destinate a governare il trattamento, che non sono derogabili dal consenso dell'interessato, e che pongono requisiti del trattamento non surrogabili dal consenso. Si può dire che esse siano poste alla stregua di requisiti di giustizia del trattamento, anche rispetto all'ipotesi di trattamento basato consenso, che siano pensate a presidio di interessi generali nel trattamento. È utile ricordare a questo proposito che il considerando 42 del Regolamento richiama la direttiva 93/13/CEE del Consiglio in materia di clausole abusive per colpire l'eventuale uso in questo contesto di clausole che determinino un significativo squilibrio tra i diritti e gli obblighi delle parti, e per ribadire la necessità di una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro, in relazione all'espressione del consenso al trattamento. Inoltre, il successivo considerando nr. 43 chiarisce che il consenso non costituisce un valido presupposto per il trattamento dei dati personali, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica. La nozione di consenso deve poi a sua volta corrispondere ai parametri fissati nell'art. 7 del regolamento già citato. Come si esprime il considerando 32 del Regolamento, il consenso deve quindi essere: "espresso mediante 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"[23]. Sulla scorta di questi principi è impensabile, ad esempio, che venga resa in Europa una sentenza simile a quella resa dalla Corte Suprema statunitense in *Sorrell v. IMS Health Care*[24] con cui la Corte ha ritenuto incostituzionale una legge del Vermont contraria alla vendita dei dati dei medici che avevano prescritto ricette portate in farmacia in difetto del consenso degli stessi medici prescrittori.

(23) Per una analisi condotta in maggiore profondità: I. Caggiano, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale*, in Annali dell'Università Suor Orsola Benincasa, 2018, consultabile sul sito: <https://www.unisob.na.it/ateneo/annali/2016-2018_1_Caggiano.pdf>; G. Resta, V Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, Riv. trim.dir. proc. civ., 2018, p. 411 ss.; S. Thobani, *I requisiti del consenso al trattamento dei dati personali*, Rimini, 2016.

(24) 564 U.S. 552 (2011). La Corte ha ritenuto che la legge non superasse lo scrutinio costituzionale rafforzato richiesto dal primo emendamento in presenza di una restrizione di: "[s]peech in aid of pharmaceutical marketing".

5. TERRENI COMUNI.

Nonostante i contrasti individuati fin qui, la comparazione tra l'esperienza europea e il diritto statunitense offre anche elementi di riflessione su alcuni punti in comune. Segnalo qui due aree nelle quale lo sviluppo di riflessioni convergenti va ormai ben al di là degli spunti occasionali.

La prima riguarda la possibilità di utilizzare la disciplina in materia di pratiche commerciali scorrette per colpire quel trattamento dati che avviene in base ad un consenso prestato dall'interessato sulla scorta di informazioni fuorvianti, decettive, ingannevoli, o di pratiche che possono dirsi altrimenti dirsi sleali, se non aggressive. L'esperienza della Federal Trade Commission in questa materia è ormai piuttosto significativa. Per risalente mandato legislativo, la Federal trade commission ha il compito di combattere pratiche di questo genere. Negli ultimi tre decenni l'Agenzia ha monitorato le pratiche commerciali che si svolgono attraverso interazioni on line per colpire quelle pratiche che, in relazione alla raccolta e alla protezione dei dati personali, sono da ritenere sleali. Non è possibile ripercorrere qui l'ampia casistica che è trattata da una letteratura recente quanto mai utile per ricostruire il quadro d'insieme[25]. Il punto è che le specifiche protezioni pensate per la tutela dei dati personali nei fatti intersecano a più riprese le norme rivolte a dettare la disciplina del mercato in termini di comportamenti conformi ad alcuni parametri di giustizia - vocabolo che non ricorre mai in questa legislazione, per ragioni fin troppo note, se non sotto le vesti ariose e leggere della fairness.

A questo riguardo, anche in Europa affiora la tendenza a monitorare l'interazione online, sulla rete per assicurare la protezione nei confronti di comportamenti commerciali scorretti che possono essere colpiti in forza delle indicazioni contenute nella Direttiva 2005/29/CE sulle pratiche commerciali scorrette e nella relativa legislazione di attuazione[26]. In Italia, la pronuncia resa dall'Autorità garante della concorrenza e del mercato nel caso WhatsApp offre indicazioni importanti circa la disponibilità di mezzi fin qui scarsamente utilizzati per reprimere pratiche commerciali che attentano agli stessi requisiti posti dalla disciplina sulla protezione dei dati personali[27].

La seconda area, connessa alla prima, è costituita dalla necessaria riflessione di fondo intorno all'autonomia del soggetto che opera on line. La stessa scelta di affidare al meccanismo del consenso la tutela dell'autonomia del soggetto può essere revocata in dubbio a fronte di *repeat players* quanto mai voraci di informazioni, che non si trovano di certo in posizione simmetrica rispetto all'individuo, né sotto il profilo dell'acquisizione dell'informazione, né quanto a capacità di gestire quanto si può ricavare dall'elaborazione dell'informazione. Questa riflessione di fondo attraversa campi diversissimi, dalla regolazione del consenso informato in medicina, alla tutela del consumatore rispetto alle clausole abusive[28]. Ha quindi perfettamente ragione Pardolesi, quando ricorda che "...puntare tutto sul recupero di un processo negoziale debitamente informato e, perciò, razionalmente capace di massimizzare il profitto congiunto, secondo i dettami della dottrina contrattuale classica, appare - a tutto concedere - velleitario. E non si vede davvero perché quest'analisi, condotta a ridosso di un'asimmetria informativa che il mercato non è in grado di correggere, non dovrebbe valere anche per il consenso al trattamento dei dati."[29].

---

(25) Per una ricostruzione dell'esperienza e della strategia messa a punto dalla Federal Trade Commission al riguardo: Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, cit., p. 145 ss.

(26) Puntualmente, in sintesi, A. De Franceschi, *La circolazione di dati personali tra* privacy *e contratto*, Napoli, 2017, spec. p. 101 ss. Indicazioni utili anche in G. Resta, e V. Zeno-Zencovich, *Volontà e consenso* cit.

(27) Il riferimento è al provvedimento dell'Autorità Garante che ha inflitto a WhatsApp Inc. una sanzione di tre milioni di euro per comunicazioni della società dirette a indurre gli utenti di WhatsApp Messenger a accettare integralmente i nuovi Termini di Utilizzo, in particolare la condivisione dei propri dati con Facebook, facendo loro credere che altrimenti sarebbe stato impossibile proseguire nell'uso dell'applicazione.

(28) Su cui voglio ricordare due interventi salienti di Roberto Pardolesi: *Clausole abusive (nei contratti dei consumatori): verso una direttiva abusata?*, in Foro it., 1994, V, 137; *Clausole abusive nei contratti dei consumatori. E oltre?* in Foro it., 2014, V, 11.

(29) S. Bonavita, R. Pardolesi, *GDPR e diritto alla cancellazione (oblio)*, cit.

Si è già detto che l'Unione europea ha maturato scelte in materia di consenso al trattamento dati più restrittive di quelle accolte negli Stati Uniti. Le imprese che operano in Europa incontrano in effetti limiti più severi nell'ottenere un consenso valido al trattamento rispetto alle loro concorrenti che si misurano sul mercato statunitense. Tuttavia anche in Europa il presidio offerto dal consenso non è poi così robusto, sopratutto se si considerano i limiti informativi, cognitivi, e strutturali che gli individui incontrano nel gestire le proprie preferenze in materia di privacy(30). Le indagini empiriche riguardanti il comportamento degli individui nelle interazioni on line confermano l'esistenza di bias cognitivi che limitano in modo sistematico e significativo la razionalità della scelta. Non mancano evidenze circa gli aspetti paradossali della condotta umana in presenza di tali limiti. È stato così rilevato che tanto più si enfatizza il messaggio secondo cui il soggetto è 'in controllo' dei propri dati personali, tanto più si manifesta la propensione a cederne il controllo ad altri(31). In questo ambiente, come è stato notato: "the subtle commodification process of personal data deregulating takes the form of contractual clauses or privacy policy declarations not known or fully understood, let alone providing accountability for actual data use"(32). Un approccio realistico alla regolazione richiede quindi lo studio delle condotte tenute in rete attraverso ricerche empiriche(33). Non è banale mettere a frutto sul piano della regolazione quanto si apprende attraverso indagini che illuminano come gli utenti si destreggiano in ambienti digitali (e come gli operatori professionali sfruttano le loro difficoltà a proprio vantaggio). Tuttavia su questo terreno l'incontro con gli studi condotti oltre oceano nella materia non prelude a collisioni: può solo servire a rendere meglio conto delle perplessità e delle critiche 'dure a morire'(34) che animano tuttora la riflessione intorno ai mezzi e agli obiettivi con cui si vuol salvaguardare l'autonomia dei privati nel mondo digitale.

(30) D. J. Solove, *Introduction: Privacy Self-management and the Consent Dilemma*, 126 Harvard Law Rev. 1880 (2013)

(31) A. Acquisti, L. Brandimarte, G. Loewenstein, *Privacy and Human Behavior in the Information Age*, in E. Selinger, J. Polonetsky, O. Tene (a cura di), *The Cambridge Handbook of Consumer Privacy*, cit., p. 184 ss., A. Acquisti, L. Brandimarte, e G. Loewenstein, *Misplaced Confidences: Privacy and the Control Paradox*, Social Psychological and Personality Science, 2013, 4(3), p. 340-347.

(32) G. Comandé, *Tortious privacy 3.0: a quest for research*, in *Essays in Honour of Huldigingsbundel vir Johann Neethling*, LexisNexis, New York, 2015, pp. 121 ss., p. 125.

(33) L. Gatt, R. Montanari, I.A. Caggiano, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale: spunti di riflessione sull'effettività della tutela dei dati personali*, Politica del diritto, 2017, p. 343 ss.

(34) Così, S. Bonavita, R. Pardolesi, *GDPR e diritto alla cancellazione (oblio)*, cit.