The God that failed. La tutela dei *co-patterners* nell'ordinamento internazionale ed europeo*

Gianpaolo Maria Ruotolo

Abstract

Il lavoro analizza le possibili forme giuridiche di tutela dei *co-patterners*, nel contesto dei "*big data* non personali", nell'ordinamento internazionale ed europeo alla luce della giurisprudenza della Corte europea dei diritti dell'uomo e di alcuni modelli normativi previsti in Europa, come la procedura dei reclami collettivi prevista dalla Carta sociale europea e alcuni meccanismi alternativi di soluzione delle controversie dell'Unione europea.

The paper analyzes the possible legal instruments of protection of co-patterners, in the context of "non-personal big data", in international and European law in the light of the case-law of the European Court of Human Rights and of some normative models offered in Europe, as the "collective complaints procedure" provided for by the European Social Charter and some European Union alternative dispute resolution mechanisms.

Sommario

Keyword

Diritto internazionale, Diritto europeo, Big Data, *Co-patterners*, *smart-cities*

* Il presente testo rappresenta una versione ampliata e con l'aggiunta delle note della relazione presentata dall'Autore alla Tavola rotonda su "*Big data*: prospettive di diritto internazionale e dell'Unione europea" svoltasi nel Dipartimento di giurisprudenza dell'Università di Ferrara il 6 giugno 2018 in occasione del Convegno nazionale della Società italiana di diritto internazionale e dell'Unione europea (SIDI).
Su determinazione della direzione, l'articolo è stato pertanto sottoposto a referaggio anonimo.

«In physics, a singularity is a point in space or time, such as the center of a black hole or the instant of the Big Bang, where mathematics breaks down and our capacity for comprehension along with it. By analogy, a singularity in human history would occur if exponential technological progress brought about such dramatic change that human affairs as we understand them today came to an end. The institutions we take for granted—the economy, the government, the law, the state—these would not survive in their present form. The most basic human values—the sanctity of life, the pursuit of happiness, the freedom to choose—these would be superseded. Our very understanding of what it means to be human—to be an individual, to be alive, to be conscious, to be part of the social order—all this would be thrown into question, not by detached philosophical reflection, but through force of circumstances, real and present».
(M. Shanahan**,** *The Technological Singularity,* Cambridge, 2015, xv)

1. Premessa

Molto frequentemente i dati vengono oggigiorno raccolti in forma "non personale", e analizzati per facilitare il monitoraggio, la sorveglianza, il controllo (come avviene nel caso di misure di sicurezza o antiterrorismo) o adottare misure di tutela di particolari interessi ritenuti prevalenti (diritti umani, epidemiologia, "*nowcasting*" di tendenze economiche). Ne vedremo più avanti, nel par. 2, alcune applicazioni nell'ordinamento internazionale.

Per il momento basti considerare che in molti casi (forse la maggior parte) i c.d. *big datasets* non sono composti di dati personali in senso stretto, cioè di dati che si riferiscono a individui determinati o determinabili nella loro univocità, e questo perché l'individuo in quanto soggetto distinto da tutti gli altri, in quanto individuo particolare insomma, non è in alcun modo utile a questo tipo di analisi, essenzialmente inferenziale, e quindi perde di centralità e rilevanza.

2. I *big data* non personali come strumento di *governance*. Alcuni profili di diritto internazionale

I dati così raccolti vengono poi analizzati al fine di costruire modelli e profili di gruppo e i risultati dell'analisi sono quindi usati per profilare situazioni generali e applicati su larga scala.

Ora, va detto che, nell'ordinamento internazionale, simili *big datasets* possono essere utilizzati sia dagli Stati sia dalle organizzazioni internazionali per programmare e valutare attività e interventi e rappresentano, quindi, un importante strumento di *governance*. Si pensi, ad esempio, alla possibilità di monitorare in tempo reale la diffusione di malattie contagiose al fine di adottare tempestivamente misure precauzionali, ai vantaggi che poterebbero derivare dalla raccolta di informazioni su una determinata patologia e sull'efficacia delle diverse terapie disponibili al fine di individuare la più efficace, alla possibilità di calcolare in tempo reale e in maniera affidabile il tasso di inflazione di una data valuta, o, ancora, di prevedere l'andamento del traffico di una metropoli[1].

[1] Sul punto si veda R. Fuller, *Structuring* Big data *to Facilitate Participation in International Law*, in *International*

Ora, la dottrina ha individuato tre distinti modelli attraverso cui i *big data* opererebbero in favore delle collettività:
1) segmentando le popolazioni in gruppi con caratteristiche omogenee rispetto a un determinato ambito, al fine di attuare interventi mirati;
2) promuovendo i principi di trasparenza e partecipazione e consentendo, in seguito all'elaborazione e quindi all'estrazione di dati inferenziali, di individuare le esigenze dei gruppi di persone così individuati per migliorare, di conseguenza, le prestazioni in loro favore;
3) sostenendo o addirittura sostituendo certe decisioni umane con algoritmi automatizzati, con conseguenti vantaggi in termini di efficienza[2].
E alcune tendenze in tal senso possono si registrano già da qualche tempo nell'ordinamento internazionale.
Si pensi, ad esempio, al progetto *Global pulse* avviato ormai quasi dieci anni or sono dal Segretariato generale delle Nazioni Unite[3], il quale mira a promuovere lo sviluppo e l'adozione su grande scala di un approccio innovativo ai *big data*, al fine di utilizzarli alla stregua di un bene pubblico, mediante il quale individuare le migliori strategie possibili di sviluppo sostenibile e azioni umanitarie: i dati, difatti, possono rappresentare uno strumento per acquisire una migliore comprensione delle variazioni del benessere umano, finanche registrando in tempo reale il *feedback* alle azioni poste in essere dalle Nazioni Unite.
Un utilizzo siffatto, seppur non esplicitamente, rievoca la possibilità di qualificare alcuni *big datasets* come beni pubblici globali[4].
Ciò potrebbe avere conseguenze giuridiche di rilievo essenzialmente sotto due profili: la natura *open* dei *big data* di rilevanza pubblica globale potrebbe modificare le condizioni di accesso ai medesimi da parte del pubblico, e, come vedremo più avanti, condurre a concepire i relativi strumenti di tutela non più in termini rigidamente individuali (poco efficaci in considerazione della perdita di rilevanza degli individui, di cui dicevamo in apertura) ma collettivi[5].

Journal of Legal Information, 2014, 504 ss. Per un accenno alle c.d. *smart cities*, v. *infra*, par. 3.

[2] «*Big data levers, such as increasing transparency and applying advanced analytics, offer the public sector a powerful arsenal of strategies and techniques for boosting productivity and achieving higher levels of efficiency and effectiveness*»; cfr. J. Manyika - M. Chui - B. Brown - J. Bughin - R. Dobbs - C. Roxburgh - A. Hung Byers, *The McKinsey Global Institute*. Big data*: the next frontier for innovation, competition, productivity*. Washington, DC, 2011, 54.

[3] www.unglobalpulse.org.

[4] Sui *global public goods* ci permettiamo di rinviare, anche solo per ulteriori riferimenti bibliografici, a G. M. Ruotolo, *Fragments of fragments. The domain name system regulation: global law or informalization of the international legal order?*, in *Computer Law & Security Review*, 2017, 159 ss., spec. 167 ss. Specificamente sul profilo accennato nel testo v. K. Śledziewska - R. Włoch, *Should We Treat* Big data *as a Public Good?*, in M. Taddeo - L. Floridi (eds.), *The Responsibilities of Online Service Providers*, Dordrecht, 2017, 263 ss.

[5] In merito alla trasparenza delle banche dati pubbliche, ricordiamo che la direttiva dell'Unione europea 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003 relativa al riutilizzo dell'informazione del settore pubblico, impone agli Stati di consentire il riutilizzo di documenti e informazioni in possesso degli enti pubblici per fini commerciali o non commerciali. Sul rapporto tra open data e diritto alla scienza, anche per ulteriori riferimenti bibliografici, ci permettiamo di rinviare a G. M. Ruotolo, *In tema di diritto alla scienza nell'ordinamento internazionale e d'istanze d'accesso aperto alla conoscenza nell'Unione europea e in Italia*, in E. Triggiani - F. Cherubini - I. Ingravallo - E. Nalin - R. Virzo (a cura di), *Dialoghi con Ugo Villani*, Bari, 2017, vol. II, 1237 ss.

In tal senso il premio Nobel per l'economia Joseph E. Stiglitz già nella prima metà degli anni '80 del secolo scorso – quando un fenomeno come i *big data* era pressoché inimmaginabile – aveva interpretato le informazioni e la conoscenza come beni pubblici, in quanto dotati delle necessarie caratteristiche («*nonrivarlous nature and nonexcludability*»)[6].
Un altro caso di utilizzo dei *big data* nell'ordinamento internazionale che rispecchia uno dei modelli illustrati – in particolare quello di cui al n. 3) della nostra precedente elencazione, di sostituzione o sostegno alle decisioni umane mediante algoritmi automatizzati – è rappresentato dal procedimento di revisione delle liste delle specie animali e vegetali alle quali garantire protezione ai sensi della Convenzione sul commercio internazionale delle specie di flora e fauna selvatiche minacciate di estinzione (*Convention on the International Trade in Endangered Species of Wild Fauna and Flora*, CITES)[7].
Tale Convenzione prevede la compilazione di liste delle specie da proteggere, soggette a revisione periodica; la revisione è effettuata dalla Conferenza dei membri della CITES[8], che agisce però sulla base di un'elaborazione matematica di enormi moli di dati che consente di tracciare le modificazioni della presenza/assenza delle varie specie protette sul territorio dei Paesi membri, mediante la costruzione di modelli di distribuzione delle specie (*species distribution modelling*, SDM).
È alla luce di tali modelli che la Conferenza CITES valuta l'opportunità di inserire o escludere dalle liste stesse una data specie[9].
Va pure segnalato, però, che, per quanto concerne l'uso dei *big data* come strumento di *governance* pubblica, l'ordinamento UE fa registrare un certo ritardo: sebbene la Commissione, già in una comunicazione del 2015 relativa a «Le piattaforme online e il mercato unico digitale. Opportunità e sfide per l'Europa», avesse auspicato «lo sviluppo di un settore pubblico basato sui dati»[10] – rifacendosi, a tal fine, anche alla Dichiarazione ministeriale "*Towards a new vision for the public sector*", adottata ad Helsinki il 28 ottobre 2015 dagli Stati membri dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE), i quali «*look forward to the strategic use of new digital tools and of Big Data to enable a data driven public sector*»[11] – ad oggi però non si registra l'adozione di strumenti normativi che impongano o promuovano un uso siffatto da parte di Istituzioni UE e Stati membri.

---

[6] Cfr. J.E. Stiglitz, *Public goods in open economies with heterogeneous individuals*, in J.F. Thisse - H.G. Zoller (eds.), *Locational analysis of public facilities*, Amsterdam/New York, 1983, 55 ss. Si vedano anche J.E. Stiglitz, *Knowledge as a global public good*, in I. Kaul - I. Grunberg - M. Stern (eds.), *Global public goods*, New York, 1999, 308 ss.; Id., *Economic foundations of intellectual property rights*, in *Duke Law Journal,* 2008, 1693 ss. Da ultimo affermano esplicitamente che «*data are—in an economic perspective—non-rivalrous and non-consumable public goods*». V. Zeno Zencovich - G. Giannone Codiglione, *Ten Legal perspectives on the "*Big data *revolution"*, in *Concorrenza e Mercato, Numero speciale su* big data *e concorrenza*, a cura di F. Di Porto, Milano, 2016, 36.

[7] *The CITES Fort Lauderdale criteria: the uses and limits on science in international conversation decision making*, in *Harvard Law Review*, 2001, 1769 ss. (curiosamente il lavoro non reca il nominativo del suo autore).

[8] L'ultima riunione della Conferenza, la diciassettesima, ha avuto luogo a Johannesburg dal 24 settembre all'8 ottobre 2016.

[9] Il database contenente la lista delle specie è consultabile su www.speciesplus.net.

[10] Doc. COM(2016) 288 final del 25 maggio 2016, 5.

[11] www.oecd.org/governance/ministerial/chair-summary-2015.pdf.

3. I rischi: influenze indebite e discriminazioni di gruppo nelle *smart cities*

Va evidenziato, poi, come i *big data* potrebbero anche essere pericolosamente utilizzati per influenzare scelte individuali di rilevanza pubblica nelle direzioni preferite dal gestore del *big dataset*.

Si pensi, ad esempio, alla c.d. *nudges theory*[12], una forma di architettura delle informazioni che mira ad alterare il comportamento delle persone in modo prevedibile, senza però proibire certe opzioni o offrire particolari incentivi[13].

Nelle sue prime modalità di applicazione questa tecnica assumeva forme piuttosto *soft*, in quanto statiche (c.d. *static nudges*, appunto, come nel caso della collocazione di merci in un certo ordine per invogliare l'acquisto di una sola di esse), ma oggi *nudges* dinamici, modificati in tempo reale sulla scorta dell'elaborazione di *big datsets*, possono essere estremamente potenti e pervasivi[14] e potrebbero essere utilizzati non solo con obiettivi commerciali, ma anche, e più pericolosamente, politici[15].

L'uso dei *big data*, poi, comporta rischi di discriminazione nei confronti dei gruppi di persone ai quali i dati si riferiscono, gruppi che vengono creati dall'algoritmo di analisi dei dati.

Ricordiamo che un determinato *dataset*, in quanto riferibile a uno specifico gruppo di individui accomunati da certe caratteristiche (i c.d. *co-patterners*, come possono essere, ad esempio i c.d. *frequent flyers* su una data tratta aerea o gli appassionati di *running* che fanno uso di strumenti di geolocalizzazione per misurare le proprie prestazioni, ma anche, sotto un differente profilo, tutte le persone che risiedono in un dato periodo in una determinata zona di una città) è idoneo, mediante la sua analisi, a individuare linee di tendenza dei comportamenti dell'intera categoria cui i dati si riferiscono.

A mero titolo di esempio si pensi al caso di un'impresa che, sulla base di elaborazioni di *big data*, resasi conto che i dipendenti che vivono più vicino al luogo di lavoro vi rimangono più a lungo di quelli che risiedono più lontano, indirizzi alla luce di questo criterio la propria politica assunzionale: ciò potrebbe condurre a un'ipotesi di discriminazione indiretta qualora le diverse zone di una città dovessero avere composizioni etniche differenti[16].

---

[12] "*Nudge*" può essere efficacemente reso in italiano con "spintarella".

[13] R. H. Thaler - C. R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness*, London, 2008, trad it. *Nudge: La spinta gentile. La nuova strategia per migliorare le nostre decisioni sul denaro, salute, felicità*, Bologna, 2014; si veda anche la recensione a tale volume di K. Yeung, *Fudge as Nudge*, in *Modern Law Review*, 2012, 122 ss.

[14] Al riguardo, in una prospettiva di *law and regulation*, si è parlato di *hypernudges*; cfr. K. Yeung, *'Hypernudge':* Big data *as a mode of regulation by design*, in *Information, Communication & Society*, 2016, 1 ss.

[15] Ricordiamo che la risoluzione del PE del 2017 sui *big data*, c. 3, lett. *f)* evidenzia i pericoli di influenza di elezioni e risultati politici tramite, ad esempio, la comunicazione mirata. Per un'analisi giuridica di un movimento politico che fa uso di elezioni online al fine di individuare i propri candidati e del possibile impatto che ciò potrebbe avere sulla democrazia nel suo complesso v. S. Curreri - S. Ceccanti, *I partiti antisistema nell'esperienza italiana: il Movimento 5 Stelle come partito personale autoescluso*, in *Diritto pubblico comparato ed europeo*, 2015, 799 ss.

[16] Si veda al riguardo il rapporto della Federal Trade Commission statunitense "Big data*: a tool for exclusion or inclusion? Understanding the issues*" del gennaio 2016, reperibile all'indirizzo www.ftc.gov.

O, ancora, si pensi al caso di *PredPol* (*Predictive Policing software*)[17], un programma sviluppato dal Dipartimento di Polizia di Los Angeles in collaborazione con University of California Los Angeles (UCLA) che è in uso da parte di molti dipartimenti di pubblica sicurezza di svariati Stati USA, il quale utilizza i *big data* per fornire previsioni su dove e quando potrebbero verificarsi crimini, al fine di prevenirli mediante il tempestivo dispiegamento delle forze di polizia. Un meccanismo analogo è stato autonomamente sviluppato anche dalla società privata *Hexagon*, che nell'ottica delle c.d. *smart cities*[18]. ha progettato un modello di ecosistema autonomo connesso (*autonomous connected ecosystem*, ACE), cioè un insieme di sistemi che si connettono tra loro e, sfruttando intelligenza artificiale e capacità di calcolo elevatissime tali da consentire di far compiere la gran parte delle analisi già ai sensori, convoglia nell'elaborazione centrale solo informazioni già raffinate, cioè inferenziali[19].

Anche predizioni di questo tipo rischiano di produrre effetti discriminatori: è accertato che l'aumentata intensità del controllo e soprattutto la sua qualità, altamente mirata quanto a modalità, tempi e luoghi specificamente suggeriti dal software (e non già, quindi, come potrebbe avvenire nel caso di un mero rafforzamento delle attività di polizia su un territorio sensibile), avviene più di frequente in zone che sono molto spesso ad alta insistenza di immigrati e minoranze etniche e linguistiche.

Va anche segnalato, per sovrappiù, come una previsione siffatta rischi di avere carattere "autoavverante", nel senso che l'aumento del numero dei crimini intercettati potrebbe essere conseguenza non già di un maggiore tasso criminale nelle zone e, soprattutto, delle minoranze sottoposte a controllo, ma della tipologia di controllo, particolarmente mirato[20].

Si pone quindi in casi siffatti un rischio di discriminazione dei *co-patterners* e, di conseguenza, la necessità di individuare forme efficaci di tutela.

4. Il problema dei dati non personali e la difficile azionabilità dei diritti del gruppo di *co-patterners*

Ora, qualora i dati analizzati per giungere alla previsione che produce effetti discriminatori fossero riferibili a individui determinati o quanto meno determinabili, costoro potrebbero beneficiare degli strumenti previsti dall'ordinamento internazionale o dagli ordinamenti interni: il quadro normativo di diritto internazionale (OCSE, Consiglio d'Europa; analogamente l'UE) relativo al trattamento dei dati è, difatti, quasi esclusivamente redatto con riguardo a informazioni personali, relative cioè a soggetti identificati o almeno identificabili.

[17] www.predpol.com.

[18] Con tale espressione, spesso resa in italiano con "città intelligente", si fa riferimento alle strategie di pianificazione urbanistica che mirano ad ottimizzare e innovare i servizi mediante il collegamento tra le infrastrutture materiali delle città mediante gli strumenti offerti dalle tecnologie della comunicazione.

[19] Disponibile all'url ww.cimdata.com .

[20] Il pensiero corre immediatamente al racconto di Philip K. Dick, *The Minority Report*, del 1956, in italiano in K. Dick, *Rapporto di minoranza e altri racconti*, (trad. di P. Prezzavento), Roma, 2004.

L'art. 4 del regolamento generale sulla protezione dei dati nell'UE[21], ad esempio, definisce tali dati come «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato")» e ritiene a tal fine «identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale». La scelta dell'ordinamento UE di far rientrare tra i dati meritevoli di tutela e nei cui confronti è possibile tutelarsi esclusivamente quelli personali rispecchia quella di altri strumenti internazionali pertinenti, come l'art. 1, lett. *b)* delle *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* adottate il 23 settembre 1980 dalla Organisation for Economic Co-operation and Development (OECD) e da ultimo aggiornate l'11 luglio 2013, che difatti definisce come "personal data" «*any information relating to an identified or identifiable individual (data subject)*»[22].

Analogamente l'art. 2 della Convenzione 108 del Consiglio d'Europa sull'elaborazione automatizzata dei dati del 28 gennaio 1981, la quale riprende pedissequamente, rendendolo però vincolante per gli Stati che hanno ratificato la Convenzione, il testo delle Linee giuda dell'OECD e definisce così "personal data" «*any information relating to an identified or identifiable individual*».

Non prevedono invece esplicitamente la necessità che i dati disciplinati siano relativi a persone identificate o identificabili le *Guidelines Concerning Computerized Personal Data Files* adottate dall'Assemblea generale delle Nazioni Unite, con la risoluzione 45/95 del 14 dicembre 1990, che contemplano una definizione di applicazione certamente più ampia della Convenzione 108 e delle *OECD Guidelines*, facendo genericamente riferimento a qualsiasi "*information about persons*"; tuttavia queste, per avendo una portata soggettiva universale, rappresentano uno strumento non vincolante.

Insomma, i paradigmi sociali, etici e, soprattutto, per quello che più ci interessa, giuridici, attualmente dominanti si concentrano principalmente sugli interessi individuali e sui danni personali prodotti dalla violazione della privacy e delle norme sulla protezione

[21] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (*general data protection regulation*, GDPR); v. L. Bolognini - E. Pelino - C. Bistolfi, *Il regolamento* privacy *europeo*, Milano, 2016; M. Krzysztofek, *Post-Reform Personal Data Protection in the European Union. General Data Protection Regulation (EU) 2016/679*, Alphen aan den Rijn, 2017; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, 2016; P. Voigt - A. von dem Bussche (eds.), *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Cham, 2017. Sull'ambito di applicazione territoriale del Regolamento ci permettiamo di rinviare a G.M. Ruotolo, *The EU data protection regime and the multilateral trading system: where dream and day unite*, in *QIL – Questions of international law*, 2018.

[22] I testi 1980 e 2013 delle linee guida sono reperibili online. L'OECD – nella consapevolezza dei rischi connessi alle differenze di regolamentazione del trattamento dei dati personali previste negli ordinamenti nazionali, che, come abbiamo già accennato, avrebbero potuto operare come barriere non tariffarie agli scambi internazionali in importanti settori dell'economia – aveva ritenuto di suggerire ai suoi Membri di armonizzare le legislazioni nazionali. P. De Hert - V. Papakonstantinou, *The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition*, in *Computer Law & Security Review*, 2014, 633 ss. Nel contesto della *mise a jour* della Convenzione si registra l'approvazione, nel febbraio 2017, da parte del Comitato consultivo della stessa, delle Linee guida sui *big data*, di cui diremo nel par. 6.

dei dati, che sono considerati diritti individuali.
Ne sia una riprova il fatto che uno dei paradigmi del legittimo trattamento dei dati è la nozione di "consenso informato", che ha senso solo se tale consenso promana dall'interessato, che è identificabile solo nel caso di dati personali.
Ma, come abbiamo visto, questo paradigma è difficilmente applicabile al caso dei *co-patterners*, i quali tuttavia potrebbero aver bisogno di tutela nei confronti di Stati, organizzazioni internazionali, soggetti privati.
Ed infatti il Comitato consultivo della Convenzione 108 del Consiglio d'Europa[23], il 23 gennaio 2017, ha adottato delle linee guida in materia di tutela delle persone con riguardo al trattamento dei dati personali nel contesto dei *big data*, che si spingono a considerare alcune peculiarità che vanno oltre le esigenze strettamente individuali che sono tradizionalmente oggetto delle norme sulla protezione dei dati personali[24].

5. La tutela nei confronti degli Stati: il modello della legittimazione dei gruppi nel contesto CEDU

La rilevanza dei gruppi, in realtà, come sappiamo, non è un fenomeno del tutto nuovo all'ordinamento internazionale: tralasciando qui la questione della rilevanza dei popoli nel contesto dell'autodeterminazione, nella costruzione dei diritti umani nel secondo dopoguerra c'era una innegabile attenzione ai "gruppi", per reazione ai regimi fascisti, e in misura minore alle dittature comuniste, che avevano negato le più fondamentali libertà di gruppi come ebrei, zingari, gay, intellettuali, borghesi.
E infatti la Dichiarazione universale dei diritti umani, il Patto internazionale sui diritti civili e politici, la Convenzione europea dei diritti dell'uomo (CEDU) rappresentano una delle reazioni giuridiche alle atrocità dei decenni precedenti.
Ora, come noto, quest'ultima, all'art. 1 obbliga gli Stati membri a garantire il rispetto dei relativi diritti a «*everyone within their jurisdiction*»; l'art. 34, come pure noto, attribuisce la legittimazione a ricorrere alla CEDU a «*any person, non-governmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto*».
Tuttavia nella prassi applicativa della CEDU questa attenzione per gli interessi generali è via via passata in secondo piano e l'attenzione si è sempre più rivolta all'individuo, ai suoi diritti e ai suoi interessi particolari.
Sappiamo, ad esempio, che gli Stati, come portatori di interessi generali, presentano ricorsi certamente con una frequenza nettamente minore rispetto agli individui; peraltro la giurisprudenza della CEDU tende a scoraggiare i ricorsi di persone giuridiche e gruppi, in particolare nel contesto dell'art. 8 della Convenzione, relativo alla tutela della vita privata, che è quello che ci interessa più da vicino.

[23] Il Comitato, la cui composizione è regolata dall'art. 18 della Convenzione 108, può fare proposte al fine di facilitare o migliorare l'applicazione della Convenzione, avanzare proposte di emendamento alla Convenzione, emette un parere su ogni proposta di emendamento che gli sia sottoposta e può, dietro domanda di una Parte, esprimere un parere su ogni questione relativa all'applicazione della Convenzione.

[24] *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of* Big data, reperibili all'indirizzo www.coe.int/data-protection.

La Corte, difatti, per lungo tempo, ha ritenuto che di norma le persone giuridiche non potessero presentare un ricorso per violazione del loro diritto alla privacy, perché quest'ultima sarebbe intrinsecamente legata ad interessi individuali e quindi, in linea di principio, patrimonio delle sole persone fisiche.
E se è vero che a partire dal 2002 la Corte ha iniziato ad ammettere le persone giuridiche a invocare il diritto alla privacy, si tratta di una giurisprudenza residuale; questi casi sono ancora l'eccezione, solo poche decine, pochissime rispetto alle migliaia di ricorsi di persone fisiche.
Peraltro, come noto, la Corte europea dei diritti dell'uomo rigetta o dichiara irricevibili i ricorsi che hanno per oggetto danni futuri o danni ipotetici, come pure inammissibile in contesto CEDU è l'*actio popularis*[25], in cui ricorrenti o gruppi di ricorrenti non intendono tutelare interessi propri, di cui sono titolari, ma interessi di altri o della società nel suo complesso (caso *Asselbourg c. Lussemburgo*[26]).
Di conseguenza gli individui possono ricorrere alla CEDU per una violazione dell'art. 8 al fine di proteggere interessi di un gruppo, solamente se tali interessi collidano con i loro o li inglobino (casi *Aksu c. Turchia*[27] e *Scozzafava e a. c. Italia*[28]).
Discorso tutto sommato analogo può esser fatto con riguardo alle persone giuridiche: di conseguenza gli individui possono anche depositare il ricorso per proteggere gli interessi delle persone giuridiche solo se i loro interessi individuali sono parte o confliggono con quelli della persona giuridica (caso *Niemetz c. Germania*[29]).
Insomma, la Corte, in massima parte, non rigetta e/o dichiara irricevibili ricorsi relativi a danni ipotetici o *in abstracto*, tranne in casi eccezionali, in cui la sua attenzione nei confronti degli interessi individuali si riduce per cosi dire, per concentrarsi su interessi

[25] La Corte internazionale di giustizia ha dato una definizione di un'azione siffatta nell'ordinamento internazionale come di quell'azione volta ad attivare «*a right resident in any member of a community to take legal action in vindication of a public interest. But although a right of this kind may be known to certain municipal systems of law, it is not known to international law as it stands at present: nor is the Court able to regard it as imported by the "general principles of law" referred to in Article 38, paragraph 1 (c), of its Statute*»; cfr. ICJ , *South West Africa, Second Phase, Judgment,* I.C.J. Reports 1966, 6. In dottrina v. W. J. Aceves, *Actio popularis. The class action in international law*, in *University of Chicago Legal Forum*, 2003, article 9.

[26] Sent. 29 giugno 1999, ric. 29121/95. La Corte in quel caso rigettò il ricorso ritenendo che dai termini "vittima" e "violazione" contenuti nell'art. 34 CEDU, come pure dall'obbligo di previo esaurimento dei mezzi di ricorso interni di cui all'art. 35, si desume che il sistema CEDU l'esercizio del diritto di ricorso individuale, oltre a non poter avere lo scopo di impedire una violazione futura della Convenzione, può esser volto solo a lamentare violazioni che riguardano il ricorrente personalmente.

[27] Sent. 15 marzo 2012, ric. 4149/04.

[28] Sent. 18 maggio 2017, ric. 20014/13. «La Corte ribadisce che per poter presentare ricorso ai sensi dell'articolo 34 della Convenzione, una persona, un'organizzazione non governativa, o un gruppo di privati deve essere in grado di sostenere di essere vittima di una violazione dei diritti riconosciuti dalla Convenzione. Per poter sostenere di essere vittima di tale violazione, una persona deve essere colpita in modo diretto dall'atto o dall'omissione in questione, o deve correre il rischio di essere colpita da esso in modo diretto (CEDU, *Monnat c. Svizzera*, ric. 73604/01 (2006), § 31). La Convenzione non prevede l'instaurazione di un'*actio popularis* per interpretare i diritti previsti da essa, né permette alle persone di contestare una disposizione della legislazione nazionale semplicemente perché ritengono, senza essere state colpite da essa in modo diretto, che essa possa violare la Convenzione».

[29] Sent. 16 dicembre 1992, ric. 13710/88. In dottrina v. W.H.A.M. van den Muijsenbergh - S. Rezai, *Corporations and the European Convention on Human Rights,* reperibile all'indirizzo www.mcgeorge.edu.

più generali: si pensi al caso *Klass ad altri c. Germania*[30], il primo in cui si solleva un'ipotesi di sorveglianza occulta di massa da parte di uno Stato, il quale si caratterizza per il fatto che i ricorrenti non erano sicuri di essere sottoposti effettivamente a un regime di sorveglianza da parte dei servizi segreti dello Stato resistente[31].
Insomma, in linea di principio, almeno, la Corte rigetta i ricorsi di persone giuridiche volti a proteggere gli interessi dei gruppi.
Al contrario consente agli individui di presentare delle azioni collettive (*class actions*) per proteggere gli interessi di un gruppo, foss'anche solo una famiglia naturale (caso *Marckx c. Belgio*[32]).
Per quanto riguarda, poi, specificamente la legittimazione dei gruppi a tutelare le loro prerogative, va detto che il sistema della Convenzione tende comunque a sollecitare che i gruppi si dotino di una posizione giuridica formalizzata, cioè che diventino delle persone giuridiche, e questo al fine di evitare dubbi in merito alla legittimazione del gruppo e di chi agisce per suo conto (si pensi, ad esempio, ai dubbi che potrebbero insorgere quando un gruppo dovesse presentare un ricorso e se, in tal caso, mancando un soggetto formalmente legittimato a rappresentarlo in toto, vi sia o meno la necessità che vi partecipi ogni singolo membro del gruppo).
La Corte, quindi, in buona sostanza rigetta i casi in cui gli individui presentano un ricorso non già in quanto direttamente interessati ma in quanto meri appartenenti al gruppo (caso *Stankov and the United Macedonian Organisation Ilinden v. Bulgaria*[33]); d'altro canto, ma l'abbiamo già detto, invece la Corte consente alle persone di presentare ricorsi cumulativi, anche quando questi riuniscono un gran numero di ricorrenti; in questi casi, tuttavia, ogni ricorrente invoca una propria posizione giuridica autonoma, seppur analoga a quella degli altri ricorrenti.

6. La "*collective complaints procedure*" della Carta sociale europea

Un meccanismo di reclami collettivi è contemplato esplicitamente, invece, dal Protocollo addizionale alla Carta Sociale Europea del 1995[34].
L'obiettivo perseguito dagli Stati membri con l'introduzione della procedura era di aumentare efficacia ed impatto della Carta e di rafforzare il ruolo delle parti sociali e delle organizzazioni non governative, consentendo loro di rivolgersi direttamente al

[30] Sent. 6 settembre 1978, ric. 5029/71.

[31] Per altri casi v. B. Van Der Sloot, *Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities*, in S. Gutwirth - R. Leenes - De Hert (eds.), *Data Protection on the Move. Current Developments in ICT and Privacy/Data Protection*, Dordrecht/Heidelberg/New York/London, 2016, 411 ss.

[32] Sent. 13 giugno 1979, ric. 6833/74.

[33] Sent. 2 ottobre 2001, ricc. 29221/95 e 29225/95.

[34] Sul punto v. R. R. Churchill - U. Khaliq, *The Collective Complaints System of the European Social Charter: An Effective Mechanism for Ensuring Compliance with Economic and Social Rights?*, in *European Journal of International Law,* 2004, 429 ss.; C. Panzera, *Diritti ineffettivi? Gli strumenti di tutela della carta sociale europea*, in *Rivista AIC*, 1, 2017, 37 ss.

Comitato europeo dei diritti sociali per lamentare la mancata attuazione della Carta da parte degli Stati che ne hanno accettato le disposizioni e, in particolare, la procedura di reclamo collettivo.

La procedura dei reclami collettivi in parola rappresenta un sistema di protezione parallelo alla protezione giudiziaria prevista dalla Convenzione europea dei diritti dell'uomo: a differenza di quanto accade alla CEDU, il Comitato europeo dei diritti sociali non può infatti esaminare ricorsi individuali, ma solo reclami collettivi presentati da organizzazioni non governative specificamente individuate dagli Stati.

Proprio in considerazione della loro natura collettiva, i reclami in parola possono essere presentati senza il previo esaurimento dei mezzi di ricorso interni e, quel che più interessa la nostra analisi, senza che l'organizzazione richiedente sia concretamente vittima della violazione contestata.

Le organizzazioni autorizzate a presentare reclami collettivi sono le seguenti: le parti sociali europee (Confederazione europea dei sindacati (CES), per i dipendenti; Business Europe e International Organization of Employers (OIE), per i datori di lavoro); alcune organizzazioni internazionali non governative che hanno uno *status* partecipativo in seno al Consiglio d'Europa; le parti sociali a livello nazionale; organizzazioni dei datori di lavoro e sindacati nel Paese interessato.

Inoltre, ogni Stato può concedere ad organizzazioni non governative nazionali rappresentative il diritto di presentare reclami; ad oggi si tratta di una facoltà esercitata solo dalla Finlandia.

Per essere dichiarato ammissibile un reclamo collettivo, tra i vari requisiti (essere firmato da una persona autorizzata a rappresentare l'organizzazione denunciante; fornire la prova che la persona che presenta e firma il reclamo ha il diritto di rappresentare l'organizzazione deve provare la rappresentatività dell'organizzazione che lo presenta; a questo proposito, il Comitato ha stabilito che, ai fini della procedura di reclamo collettivo, la rappresentatività è un concetto autonomo, non necessariamente identico alla nozione nazionale di rappresentatività[35] e che qualora il denunciante sia una ONG internazionale o nazionale, va fornita la prova che l'organizzazione denunziante ha una competenza specifica nel settore relativo alle disposizioni della Carta oggetto della denuncia.

Insomma, anche questo modello presuppone un'importante formalizzazione della struttura di rappresentanza dei gruppi e, come già il modello CEDU, consente solo il ricorso nei confronti di soggetti statali, impedendo di reagire a comportamenti di privati.

7. Modelli sostanziali di tutela delle posizioni giuridiche dei gruppi utilizzabili (anche) nei confronti di privati

Insomma, i modelli (processuali) fin qui delineati non appaiono idonei a disciplinare compiutamente i profili di tutela dai e dei *big datasets* non personali.

[35] *Confédération française de l'Encadrement "CFE-CGC" c. France*, reclamo n. 9/2000, decisione sull'ammissibilità del 6 novembre 2000, § 6, reperibile all'indirizzo www.coe.int.

Proviamo ora a cercare di individuare dei modelli, relativi stavolta a posizioni giuridiche sostanziali, da invocare dinanzi alle giurisdizioni interne, a tal fine.
Ciò ci consentirebbe non solo di risolvere i problemi di legittimazione dei gruppi delineati nei paragrafi precedenti, ma anche di concepire una tutela nei confronti dei privati, impossibile mediante i meccanismi puramente interstatali sin qui descritti.
Un primo modello che è stato utilizzato per cercare di costruire una forma di tutela dei gruppi è quello dei diritti delle minoranze[36]; ora, tali diritti sono essenzialmente basati sul divieto di discriminazione (la cui violazione, come abbiamo già visto nel par. 3, è uno dei rischi dell'abuso di *big datasets*). D'altro canto siffatti diritti presuppongono l'esistenza della minoranza, cioè del gruppo da tutelare, il quale è già formato prima che i suoi diritti vengano invocati, ciò che invece non avviene nel caso dei gruppi di *co-patterners*, che vengono in essere, per il tramite dell'algoritmo che, analizzando il *dataset*, li crea.
Un altro modello utilizzabile potrebbe essere quello della c.d. *relational privacy* (spesso definita anche "*family privacy*")[37]: l'idea è che gruppi come la famiglia formerebbero un'unità legittimata in quanto tale a tutelare la sua stessa riservatezza e, più in generale, le sue posizioni giuridiche. Tuttavia in questo caso il gruppo in questione, la famiglia, troverebbe con facilità un legale rappresentante, problema che, come abbiamo già visto, è invece con grande difficoltà risolvibile nel caso dei gruppi di *co-patterners*.
Il terzo modello che si potrebbe pensare di utilizzare è quello della c.d. tutela delle generazioni future e dei loro diritti, spesso invocata nel contesto del diritto internazionale dell'ambiente[38]: si discute difatti anche in questo caso, come in quello dei *co-patterners*, di raggruppamenti di persone non ancora esistenti nel momento in cui se ne invocano i diritti. Va però detto che la letteratura che si occupa dei diritti delle generazioni future, essenzialmente, si focalizza sugli obblighi delle generazioni attuali a preservare gli interessi di quelle future, le quali, sotto il profilo giuridico assumono quindi scarsa rilevanza: si tratta di una circostanza che rende difficilmente adattabile anche questo modello al problema di cui ci stiamo occupando.
Il quarto modello giuridico utilizzabile potrebbe essere quello del diritto a non nascere ("*wrongful life/birth*"), che in questo caso potrebbe essere applicato al gruppo in quanto tale, la cui "nascita" sarebbe fonte di discriminazione e/o danno; siamo perfettamente consapevoli, tuttavia, come l'esistenza stessa della posizione giuridica in parola sia contestata[39]. Rimarrebbe anche in questo caso comunque irrisolto il problema della rappresentanza del gruppo di *co-patterners*.

---

[36] Per alcuni riferimenti v. P. Torretta*, Diritti fondamentali e protezione delle "istanze collettive di diversità": il caso delle minoranze linguistiche*, in *Diritto pubblico comparato ed europeo*, 2014, 695 ss.

[37] R.H. Sloan - R. Warner, *Relational Privacy: Surveillance, Common Knowledge, and Coordination*, in *The University of St. Thomas Journal of Law & Public Policy*, 2017.

[38] Anche per ulteriori riferimenti bibliografici v. D. A. Farber, *From Here to Eternity: Environmental Law and Future Generations*, in *University of Illinois Law Review*, 2003, 2899 ss.

[39] La Cassazione italiana a sezioni unite, ad esempio, con sentenza n. 25767 del 22 dicembre 2015 ha risolto un contrasto giurisprudenziale sulla responsabilità medica per nascita indesiderata negando il risarcimento per i danni da "vita ingiusta" subiti dalla figlia e accogliendo invece la richiesta del risarcimento del danno patito dai genitori.

8. I *big datasets* non personali nell'UE: difficoltà giurisdizionali e un'ipotesi di ADR

Anche il contesto dell'Unione europea, pur più evoluto rispetto all'ordinamento internazionale, soffre una sorta di inadeguatezza normativa in qualche misura paragonabile a quelle sin qui descritte.

Sebbene la Commissione abbia recentemente avanzato una proposta di regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea[40], la stessa, pur riconoscendo alcune delle peculiarità di tali dati, però, si concentra esclusivamente, come già evidente già dal titolo, sui problemi della loro circolazione, senza preoccuparsi dei connessi profili di tutela.

Eppure il Parlamento europeo ha già evidenziato come, a causa delle quantità di dati e dei sistemi utilizzati per la loro analisi, i *big data* possano «condurre non solo a violazioni dei diritti fondamentali dei singoli, ma anche a una disparità di trattamento e a una discriminazione indiretta nei confronti di gruppi di persone con caratteristiche simili, in particolare per quanto concerne l'equità e le pari opportunità di accesso all'istruzione e all'occupazione, quando si offre un lavoro alla persona o la si valuta oppure quando si determinano le nuove abitudini di consumo degli utenti dei media sociali»[41]. Di recente, poi, la Corte di giustizia ha deciso una questione pregiudiziale relativa all'ammissibilità di una sorta di ricorso collettivo contro Facebook[42]: nella causa *a quo* il solito Maximilian Schrems[43] aveva agito dinanzi a una Corte austriaca per la tutela sua

---

[40] Si veda il doc. COM(2017)495 final del 13 settembre 2017.

[41] Risoluzione cit. *supra,* nota 48, punto 19, i corsivi sono nostri.

[42] CGUE, C-498/16, *Schrems c. Facebook Ireland Limited* (2018).

[43] Si tratta del medesimo individuo il cui ricorso dinanzi alla High Court irlandese aveva generato il rinvio pregiudiziale all'esito del quale la Corte aveva poi annullato la decisione 2000/520/CE della Commissione, del 26 luglio 2000, adottata in applicazione della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti; cfr. CGUE, C-362/14, *Maximillian Schrems c. Data Protection Commission* (2015). In dottrina v. R. Bifulco, *La sentenza Schrems e la costruzione del diritto europeo alla "privacy" – Nota a CGUE Grande sezione 6 ottobre 2015 (causa C-362/14)*, in *Giurisprudenza costituzionale*, 2016, 289 ss.; B. Carotti, *Il caso "Schrems", o del conflitto tra riservatezza e sorveglianza di massa*, in *Giornale di diritto amministrativo*, 2016, 333 ss.; S. Crespi, *Il trasferimento dei dati personali UE in Stati terzi: dall'Approdo sicuro allo Scudo UE/USA per la "privacy"*, in *Diritto pubblico comparato ed europeo*, 2016, 687 ss.; G. Finocchiaro, *La giurisprudenza della Corte di giustizia in materia di dati personali da "Google Spain" a "Schrems"* in *Il Diritto dell'informazione e dell'informatica*, 2015, 779 ss.; A. Giattini, *La tutela dei dati personali davanti alla Corte di giustizia dell'UE: il caso "Schrems" e l'invalidità del sistema di "approdo sicuro"*, in *Diritti umani e diritto internazionale*, 2016, 247 ss.; M. Mastracci, *Evoluzione del diritto alla privacy tra Europa e Stati Uniti: dal Safe Harbor al Privacy Shield*, in *La Comunità internazionale*, 2016, 555 ss.; A. Mantelero, *From "Safe Harbour" to "Privacy Shield". The "medieval" sovereignty on personal data*, in *Contratto e impresa. Europa*, 2016, 338 ss.; Id., *Il trattamento dati nelle imprese nel post "Safe Harbour". Strategie di breve, medio e lungo periodo*, in *Il Diritto dell'informazione e dell'informatica*, 2015, 887 ss.; M. Nino, *La Corte di giustizia UE dichiara l'invalidità del sistema di* Safe Harbour: *la sentenza* Schrems, in *Quaderni di Sidiblog*, Napoli, 2015, 286 ss., reperibile online all'indirizzo www.sidiblog.org; Id., *Le prospettive internazionali ed europee della tutela della privacy e dei dati personali dopo la decisione* Schrems *della Corte di giustizia UE*, in *Il Diritto dell'Unione eu*ropea, 2016, 755 ss.; P. Piroddi, *I trasferimenti di dati personali verso paesi terzi dopo la sentenza "Schrems" e nel nuovo regolamento generale sulla protezione dei dati*, in *Il Diritto dell'informazione e dell'informatica*, 2015, 827 ss.; F. Rossi Dal Pozzo, *La tutela dei dati personali*, cit., in *Rivista di diritto internazionale*, 2016, 690 ss.; G. Scarchillo, *Dal Safe Harbor al Privacy Shield. Il trasferimento di dati personali verso gli Stati Uniti dopo la sentenza Schrems*, in *Diritto del commercio internazionale*, 2016, 901 ss.; S. Sica - V. D'Antonio, *I "Safe Harbour Privacy Principles": genesi,*

e di altre persone[44] contro il social network, accusato di aver applicato in maniera massiva politiche illegittime di raccolta, elaborazione e condivisione di dati, nonché di aver fornito i risultati delle proprie elaborazioni – sia in senso individuale sia, per quanto interessa più da vicino la nostra analisi, in senso aggregato – al Governo USA per i suoi programmi di sorveglianza di massa, in particolare il famigerato PRISM.
La Corte austriaca chiedeva quindi alla Corte di giustizia di chiarire se il regolamento (CE) 44/2001, c.d. Bruxelles I, *ratione temporis* applicabile, concernente, come noto, la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, e, in particolare, l'art. 16, par. 1[45], potesse essere interpretato nel senso di consentire ad un singolo di far valere all'interno di uno Stato membro, contestualmente ai *propri*, anche diritti analoghi di *altri* consumatori, i cui dati fossero stati aggregati.
Va chiarito che nel procedimento *a quo* l'attore si era premurato di farsi cedere da tali altri interessati i loro diritti, proprio al fine di proporre l'azione giurisdizionale "collettiva", e tale cessione fosse da costoro stata concessa proprio al fine di garantire un esercizio *generale* dei diritti coinvolti nell'azione proposta.
Nelle sue Conclusioni, presentate il 14 novembre 2017, l'Avvocato generale Michal Bobek suggeriva alla Corte di dichiarare che, alla luce dello stato attuale del diritto UE e, in particolare dell'art. 16, par. 1, del reg. Bruxelles I, un consumatore non può far valere, contemporaneamente a diritti propri, diritti aventi lo stesso oggetto che gli siano a tal fine stati ceduti da altri consumatori domiciliati in altre località all'interno dello stesso Stato membro, in altri Stati membri o in Paesi terzi.
L'A.G., infatti, pur riconoscendo l'opportunità di prevedere la possibilità di azioni collettive all'interno dell'Unione, ricordava che, a parte alcuni strumenti di diritto non vincolante, di cui diremo fra poco, l'ordinamento UE non contempla una siffatta possibilità, la quale non potrebbe, quindi, essere riconosciuta per via giurisprudenziale, necessitando invece di un intervento legislativo organico[46].
Ed è esattamente quello che ha fatto la Corte il 25 gennaio 2018, dichiarando che, allo stato, l'ordinamento UE non conosce tale possibilità.
Insomma, per quanto riguarda la tutela collettiva di lesioni di interessi che colpiscono gruppi di *co-patterners* in conseguenza del trattamento *in blocco* di dati non personali, l'or-

contenuti, criticità, in *Il Diritto dell'informazione e dell'informatica*, 2015, 801 ss.; V. Zeno-Zencovich, *Intorno alla decisione nel caso "Schrems": la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, *ivi*, 2015, 683 ss.

[44] Sebbene il procedimento pendente dinanzi al giudice del rinvio riguardasse soltanto sette consumatori domiciliati in Austria, Germania e India, successivamente più di 50.000 persone avevano provveduto a cedere a Schrems i loro diritti nei confronti di Facebook mediante un sito web volto alla raccolta della volontà degli interessati: www.fbclaim.com.

[45] «L'azione del consumatore contro l'altra parte del contratto può essere proposta o davanti ai giudici dello Stato membro nel cui territorio è domiciliata tale parte, o davanti ai giudici del luogo in cui è domiciliato il consumatore». Ricordiamo che, a partire dal 10 gennaio 2015, il regolamento 44/2001 è stato sostituito dal reg. 1215/2012, il cui art. 18, par. 1, prevede che «l'azione del consumatore contro l'altra parte del contratto può essere proposta davanti alle autorità giurisdizionali dello Stato membro in cui è domiciliata tale parte o, indipendentemente dal domicilio dell'altra parte, davanti alle autorità giurisdizionali del luogo in cui è domiciliato il consumatore».

[46] Cfr. il par. 123 delle Conclusioni cit.

dinamento internazionale e l'ordinamento UE dimostrano di essere in uno stallo, una sorta di singolarità nel senso esplicitato da Shanahan nel passaggio citato come *incipit* di questo lavoro, in cui i meccanismi di tutela giuridica normalmente predisposti non appaiono in grado di funzionare.

Il dio ha fallito, insomma.

De jure condendo ricordiamo, tuttavia, che la Commissione ha, qualche tempo addietro, adottato una raccomandazione relativa ai «principi comuni per i meccanismi di ricorso collettivo di natura inibitoria e risarcitoria negli Stati membri che riguardano violazioni di diritti conferiti dalle norme dell'Unione»[47] che, per quanto concerne la legittimazione ad agire, suggerisce agli Stati membri di designare delle organizzazioni che possano intentare azioni rappresentative di una pluralità di individui con interessi comuni[48].

Si tratta di un'idea che potrebbe essere in qualche modo recuperata con riferimento al caso in esame: una individuazione preventiva di organizzazioni indipendenti legittimate ad agire per la tutela dei gruppi di *co-patterners* potrebbe infatti superare almeno alcune delle difficoltà fin qui tracciate.

E, al riguardo, di fianco alla legittimazione ad azioni in sede giurisdizionale, forse ancor più efficace potrebbe essere la previsione di meccanismi di *alternative dispute resolution* analoghi a quelli previsti nel regolamento (UE) 524/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo alla risoluzione delle controversie *online* dei consumatori e che modifica il regolamento (CE) 2006/2004 e la direttiva 2009/22/CE (regolamento sull'ODR per i consumatori)[49].

---

[47] Raccomandazione 2013/396/UE dell'11 giugno 2013. Si vedano in dottrina R. Cisotta, *The Evolving Framework for Antitrust Damages Actions and Collective Redress in the European Union: a First Assessment*, in *Diritto del commercio internazionale*, 2014, 709 ss.; M. Danov, *The Brussels I Regulation: Cross-Border Collective Redress Proceedings and Judgments*, in *Journal of Private International Law*, 2010, 359 ss.; B. Hess, *Collective Redress and the Jurisdictional Model of the Brussels I Regulation*, in A. Nuyts - N.E. Hatzimihail (eds.), *Cross-Border Class Actions. The European Way*, Munich, 2014, 59 ss.; E. Lein, *Cross-Border Collective Redress and Jurisdiction under Brussels I: a mismatch*, in D. Fairgrieve - E. Lein (eds.), *Extraterritoriality and Collective Redress*, Oxford, 2012, 129 ss.; A. Nuyts, *The Consolidation of Collective Claims under Brussels I*, in A. Nuyts - N.E. Hatzimihail (eds.), *op. cit.,* 69; Z.S. Tang, *Consumer Collective Redress in European Private International Law*, in *Journal of Private international Law*, 2011, 101 ss.; Id., *Electronic Consumer Contracts in the Conflict of Laws*, Oxford, 2015, 284 ss.; A.M. Romito, *I provvedimenti inibitori a favore del consumatore nella disciplina dell'Unione europea*, in *Studi sull'integrazione europea*, 2014, 503 ss.

[48] La raccomandazione auspica che siffatte organizzazioni non abbiano scopo di lucro, che vi sia un nesso diretto tra i loro obiettivi principali e i diritti conferiti dalle norme dell'Unione di cui si lamenta la violazione per i quali l'azione è esperita e che le stesse abbiano sufficienti capacità, in termini di risorse finanziarie e umane e di competenza legale, per rappresentare una molteplicità di ricorrenti agendo nel loro interesse.

[49] Per un'analisi diffusa dei meccanismi ivi previsti, certamente ultronea in questo contesto, ci permettiamo di rinviare a G.M. Ruotolo, *La soluzione delle controversie online dei consumatori nell'Unione europea tra armonizzazione e diritto internazionale privato*, in *Studi sull'integrazione europea*, 2015, 359 ss.