Giovanna De Minico

Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria

(doi: 10.1438/93721)

Diritto pubblico (ISSN 1721-8985)
Fascicolo 1, gennaio-aprile 2019

Ente di afferenza:
Universit Napoli Federico II (unina)

Giovanna De Minico

Big Data e la debole resistenza delle categorie giuridiche

Privacy e *lex mercatoria*

Sommario: 1. I *Big Data* e le categorie del diritto. – 2. Il diritto alla privacy e i *Big Data.* – 3. La definizione del rapporto privacy/*Big Data* nel Regolamento 2016/679. – 4. I *Big Data*: una continuità discontinua con la *lex mercatoria*. – 5. Gli impegni vincolanti al tempo dell'economia *data driven.* – 6. E il cerchio si potrebbe chiudere a condizione di …

1. *I* Big Data *e le categorie del diritto*

Il tema dei *Big Data*[1] rende visibile la forza corrosiva di Internet che distrugge, modifica e crea nuove categorie giuridiche secondo un ritmo continuo e discontinuo, prevedibile e imprevedibile. Gli antichi paradigmi cedono il posto ai nuovi che il decisore politico disegnerà in coerenza con gli obiettivi della regolazione. Qui si è scelta l'uguaglianza sostanziale come *focus* di questo disegno in antitesi alla conservazione dello *status quo,* che non consente agli esclusi nel godimento dei diritti economici o nella partecipazione alle libertà politiche di allinearsi con i più fortunati. Chi dovesse assumere una finalità diversa, perverrà a esiti regolatori presumibilmente distanti dai nostri, risultato inevitabile quando la scelta è politica, quindi opinabile.

Prima di esaminare la tipologia di categorie giuridiche destrutturate dai BD intendiamoci sul loro significato.

Il termine si riferisce a masse enormi di dati universali per oggetto e soggetto, variabili per capacità auto-generativa, veloci per la formazione *in progress* del patrimonio informativo. Sulla *querelle* definitoria la dottrina

[1] Da ora in avanti useremo l'acronimo BD. F.X. Diebold, *A personal perspective on the origin (s) and development of "Big Data": the phenomenon, the term, and the discipline*, PIER Working Paper No. 13-003, 2012, in *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2202843.*

 ISSN 1721-8985

americana[2] si diceva soddisfatta dalle quattro V, in seguito è ricorsa a una quinta "v", quella del valore, economicamente inestimabile, anche se questa non è una buona ragione per negare loro questo attributo[3]. Non è da escludere in avvenire che altre lettere si aggiungano alle prime.

Da un'ottica economica, i BD rappresentano il nuovo *asset* delle imprese operanti in rete, un'*essential facility* secondo l'accezione della Corte di giustizia[4], non diversamente da quanto lo sia stata la rete fissa per le Telco, fermo restando le diversità tra i due termini. La rete è il risultato d'investimenti, cioè esiste grazie all'impiego di energie economiche del suo *dominus*; queste masse di dati invece sono create dai cittadini della rete, che con noncuranza lasciano pezzi di sé durante la navigazione. Sta accadendo in Internet quanto capitava a Pollicino, che nell'attraversare il bosco lasciava cadere a terra briciole di pane per ritrovare la via di casa. Anche noi durante la navigazione lasciamo cadere frammenti della nostra identità, che raccolti e riorganizzati da chi verrà dopo comporranno il patrimonio virtuale della sua attività d'impresa, cioè gioveranno fondamentalmente a chi li ha raccolti, non alla persona alla quale i dati appartenevano.

Questa genesi fa dubitare della legittimità di atteggiamenti proprietari sui dati da parte da chi li utilizza per fini lucrativi, perché reclamare posizioni di esclusiva è incompatibile con la terzietà dei beni rispetto al patrimonio del rivendicante; lì dove le uniche pretese azionabili sono simili a quelle del depositario di un bene altrui, con la conseguente preclusione di ogni aspettativa dominicale sui BD.

Ora possiamo osservare cosa accade quando il nuovo fenomeno dei BD incontra le categorie giuridiche del diritto alla privacy e della *lex mercatoria*. Queste ultime rimangono invariate? E, in caso di esito negativo alla domanda, in che misura i BD alterano i rispettivi paradigmi?

[2] D. Laney*, 3-D data management: controlling data volume, velocity and variety*, 2001, *https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.*

[3] J. Gantz, D. Reinsel, *Extracting value form chaos,* in *IDC iView*, 2011, in *http:// www.emc.com/collater/analyst-reports/idc-extracting-value-fdrom-chaos-ar.pdf*; B. Marr, *Big data: The 5 V everyone must know, 2014*, in *https://www.linkedin.com/pulse/20140306073407-64875646-big-data-the-5-vs-everyone-must-know.*

[4] Cfr.: *Case C-418/01, IMS Health GmbH 6Co. OHG v. NDC Health Gmh & Co. Kg* (2004), in *ECLI*, UE, 2004, p. 257; *Case C-7/97, Oscar Bronner Gmh& Co. KG v. Mediaprint Zeitungs-und Zeitschriftenverlag GmbH 6Co. KG, Mediaprint*, in *ECLI, EU,* 1998, p. 569.

2. *Il diritto alla privacy e i* Big Data

Faremo precedere il discorso sulle nuove coordinate del rapporto BD/privacy ritornando indietro nel tempo per riprendere per punti essenziali l'evoluzione del diritto alla privacy nella misura in cui questo *flash* sia utile al nostro obiettivo.

Il suo originario abito era disegnato sul modello del diritto di proprietà[5], che dilatava il suo oggetto dalle *res* materiali al foro interno dell'individuo. Questa categoria giuridica si rivelò presto inadeguata rispetto a una privacy irrinunciabile dal suo titolare perché bene essenziale allo sviluppo della persona, contro la piena disponibilità del diritto reale; la natura antitetica delle due situazioni soggettive e dei rispettivi regimi giuridici era la prova dell'estraneità della privacy al *genus* dominicale.

Saltiamo in questa sede i passaggi intermedi[6] meritevoli però di aver sottratto la privacy ai diritti patrimoniali per attrarla all'area delle libertà fondamentali con tutto ciò che ne segue[7]. Arriviamo invece alla bella proposta di Rodotà[8], che proietta il diritto in esame nello scenario tecnologico, valorizzandolo come pretesa all'autodeterminazione della propria immagine digitale. Questa nuova qualificazione segna un salto di qualità: da una privacy gelosamente custodita nel cassetto del titolare a diritto che si snoda giorno dopo giorno in un flusso verso l'esterno volontario, continuativo e crescente di dati. Questa nuova dimensione riconosce all'individuo, non il semplice diritto di essere lasciato in pace, ma quello di controllare l'esattezza dei dati che lui stesso ha esternato e, se del caso, anche di correggerli, potendo da ultimo avere un interesse qualificato a cancellare quanto di sé aveva un tempo reso pubblico.

Anche questa dimensione bilaterale della privacy blocca però il diritto in un ambiente ancora conoscibile alla persona e quindi non coglie la sua propensione a confrontarsi con la sfida tecnologica imposta dall'*habitat* digitale e dalle analisi predittive degli algoritmi.

[5] S.D. Warren, L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, IV, 5, p. 189, anche in *https://www.stetson.edu/law/studyabroad/netherlands/media/Trk1.Week3-Bauer-Tuesday-Warren-and-Brandeis-Right-to-Privacy-1890-Harvard-Law-Review.pdf.*

[6] M. Orofino, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *Riv. Dir. Media*, 2, 2018, pp. 9 ss.

[7] D.J. Solove, *Conceptualizing Privacy*, in *California Law Review*, 20, 2002, p. 1088.

[8] S. Rodotà, *Tecnologia e diritti,* Bologna, Il Mulino, 1995, capp. 2 e 3.

In questa terza ulteriore fase[9] il soggetto non trova gli strumenti idonei per proteggere una privacy destrutturata nella borsa degli attrezzi del diritto all'autodeterminazione: le antiche forme di tutela basate sul consenso informato si rivelano ben presto insufficienti e inadatte al mutato terreno di gioco. Invero, i dati raccolti in forma massiva sono tendenzialmente anonimi e quindi non hanno un titolare, individuato o individuabile, legittimato a prestare il consenso; ma anche nell'ipotesi in cui i dati avessero un nome e un cognome, chi li raccoglie non può sapere in quel momento quale sarà il loro impiego futuro. Quindi, chi colleziona dati con la rete a strascico non ci può dire per quale finalità li sta affastellando, perché lo ignora anche lui, e se pure conoscesse lo scopo della raccolta, nulla ne impedirebbe l'impiego successivo per fini diversi da quelli iniziali. Una cosa è certa: i dati non rimarranno fermi perché rappresentano il punto di avvio delle analisi predittive, cioè di quelle attività previsionali dirette ad anticipare con prognosi *ex ante* le condotte che intere categorie di soggetti presumibilmente assumeranno secondo le proiezioni dell'algoritmo.

Pertanto, nelle condizioni di buio totale il nostro consenso[10] informato è diventato un «non consenso». Questo spiega perché l'antica tutela della privacy, *consent based*, assistita dalle garanzie dell'autonomia e della consapevolezza, non è più utilmente invocabile. Entrambi questi attributi si sono sbriciolati dinanzi ad assensi estorti con la coercizione psicologica di negare il servizio digitale a chi si fosse rifiutato di cedere i dati o li avesse ceduti senza cognizione di causa nell'ignoranza piena delle finalità del loro impiego.

Chiarito che la privacy non è più il diritto che era un tempo, definiamo secondo un approccio fattuale quale sia la nuova posizione del titolare dei dati. Questi pretende di avere un ruolo attivo nel processo di *predictability*[11] della sua condotta al fine di controllarne gli esiti previsionali, e per fare ciò deve chiedere almeno due cose: visibilità relativa dell'algoritmo e imputazione *sui generis* della responsabilità civile.

Quanto alla trasparenza funzionale dell'algoritmo, essa è soddisfatta in presenza di una sua *disclosure* selettiva, cioè idonea a coprire solo le linee portanti dell'algoritmo per consentire agli interessati di comprendere

[9] V. Mayer, S.K. Cukier, *Big Data*, Boston, Hartcourt Publishing Company, 2013 (trad. it. Garzanti, 2013), cap. 9.

[10] W. Kerber, *Digital markets, data and privacy: competition law, consumer law and data protection*, in *GRUN int*, 2016, pp. 641 ss.

[11] E. Siegel, *Predictive Analytics: the power to predict who will click, buy, lie or die*, (revised), New Jersey, Wiley, 2016, pp. 91 ss.

i fini ultimi del meccanismo predittivo. Del resto una conoscenza completa azzererebbe ingiustificatamente il diritto di proprietà intellettuale del suo legittimo titolare senza neppure giovare allo scopo informativo perché rendere pubblico il funzionamento integrale di un algoritmo è comprensibile solo a pochi addetti ai lavori. Quindi, questa posizione estrema creerebbe un danno senza procurare alcun vantaggio: viziata per difetto di necessità e di proporzionalità, va scartata.

La seconda pretesa è conseguibile a condizione di chiamare in causa il diritto civile per disegnare un criterio nuovo di imputazione della responsabilità, in caso di previsione dannosa perché discriminatoria verso talune categorie sociali o perché basata su calcoli rivelatisi erronei. Da qui la necessità di sostituire al criterio civilistico di imputazione per colpa un parametro indipendente dalla diligenza e avente il suo titolo giustificativo nel rischio di impresa; in questo modo la collettività danneggiata avrebbe comunque un responsabile cui rivolgersi per il ristoro dei danni per il fatto oggettivo che l'evento pregiudizievole si è avverato, indipendentemente dal giudizio sulla sua riferibilità psicologica alla condotta del responsabile.

Da quanto detto la privacy vede svanire la sua iniziale dimensione bilaterale nel momento in cui si sposta in un contesto soggettivo trilaterale, dove al titolare dei dati e al responsabile del trattamento si è aggiunto l'autore dell'algoritmo o il suo utilizzatore, nei confronti del quale sarà azionabile la pretesa all'intellegibilità del meccanismo predittivo.

3. *La definizione del rapporto privacy/*Big Data *nel Regolamento UE 2016/679*

Sul punto centrale privacy/prevedibilità dell'algoritmo il recente Regolamento europeo[12] è latitante. Non tanto perché le espressioni BD o intelligenza artificiale non ricorrano nel testo, *consideranda* inclusi, quanto per il modo in cui il legislatore europeo ha risolto l'interrogativo su come valutare il rischio inerente alle analisi predittive. Non anticipiamo giudizi se non dopo aver esaminato il dato di diritto positivo.

[12] Regolamento Europeo 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», nonché in adeguamento il D.Lgs. 10/8/2018, n. 101. D'ora in avanti, Reg.

Il Regolamento, pur meritevole di apprezzamento[13] nelle parti sulla *privacy by design* o *by default*, o nelle *querelle* sulla portabilità dei dati da una piattaforma all'altra, conserva invece un atteggiamento nostalgico verso la privacy, costretta ancora a prestare omaggio al bilateralismo arcaico *ante* Internet, protetta in quello scambio consenso informato/dati personali che, già prima dell'avvento dei BD, realizzava una finta difesa piuttosto che una forma di tutela effettiva per le ragioni già esposte sopra.

La soluzione ideata dal legislatore europeo consiglia o impone, a seconda dei casi, alle imprese con vocazione al trattamento dei dati di compilare una valutazione di impatto sulla privacy (art. 35 Reg.). In estrema sintesi questa valutazione consiste nell'analizzare *ex ante* i rischi elevati che l'aggregazione dei dati potrebbe «comportare per gli interessi e le libertà delle persone fisiche» (art. 35) e quindi nel prevedere le misure organizzative e comportamentali più adatte a evitarli. Rischi e rimedi sono individuabili grazie ai nove criteri consegnati nelle Linee guida dei Garanti europei[14], nonché al concerto delle Autorità garanti nazionali a vario titolo chiamate in causa.

Questo sistema denuncia almeno quattro criticità[15].

La prima attiene alla circostanza che i rischi di facile individuazione si riducono alla lesione dell'integrità delle banche dati, alle intromissioni e violazioni interne o esterne, trascurando il vero pericolo connesso ai BD: i dati aggregati, che, se usati da un algoritmo come materiale grezzo, sono suscettibili di provocare valutazioni pregiudizievoli per diffuse categorie di soggetti. Ebbene, al momento di questa valutazione il rischio da previsione comportamentale rimane la vera incognita, perché è inimmaginabile in

[13] M. Orefice, *Artificial intelligence and the right to privacy in the times of terrorism*, in G. De Minico, O. Pollicino (eds.), *Virtual Freedoms – Terrorism – The Law*, in corso di pubblicazione, London, Routledge, 2019.

[14] Gruppo di lavoro articolo 29 per la protezione dei dati, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*, 4 aprile 2017, in *http://www.besantsrl.it/sito-wp/wp-content/uploads/2018/03/Linee-guida-concernenti-valutazione-impatto-sulla-protezione-dati.pdf*.

[15] *Contra*: L. Califano, *Il regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali*, in L. Califano, C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona*, Napoli, Editoriale Scientifica, 2017, pp. 35 ss.; S. Calzolaio, L. Ferola, V. Fiorillo, E.A. Rossi, M. Timiani, *La responsabilità e la sicurezza del trattamento*, in L. Califano, C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona*, cit., pp. 178-186 e F. Pizzetti, *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in F. Pizzetti (a cura di), *Intelligenza artificiale protezione dei dati e regolazione*, Torino, Giappichelli, 2018, p. 74.

cosa possa consistere, quale la sua gravità, quando possa verificarsi e chi possa pregiudicare. Ne consegue che nessun rimedio anticipato sarebbe proponibile per scongiurarne l'avveramento perché si avrà contezza del rischio solo a fatto compiuto. Né i nove criteri possono fare luce sull'*ubi consistam* del pericolo, perché significherebbe pretendere dalle persone capacità divinatorie. Ne siano prova le Linee guida che si dilungano solo sugli aspetti marginali della valutazione senza neppure riuscire a definire i tanti elementi indeterminati della fattispecie giuridica – quale il concetto di sua notevole entità – che necessiterebbero un chiarimento ai fini della certezza del diritto. Quindi, si faccia o no questa valutazione, la situazione non cambia in termini di tutela anticipata della collettività: il rischio rimane fuori da questa assicurazione collettiva, anche se doveva essere il vero pericolo da cui difendersi.

La seconda obiezione è che la valutazione riguarderebbe dati personali, cioè riferibili a un titolare, quindi non i BD, che lavorano tendenzialmente su dati anonimi. A ciò si potrebbe obiettare che l'anonimato diffuso dei BD esclude che qualcuno possa avere un motivo giuridico di doglianza visto che le previsioni dannose interesseranno soggetti non identificabili. Ma questa eccezione non tiene conto della circostanza che i BD usano dati anonimi, che a seguito di incroci sinergici tra più banche diventano riferibili a persone. Solo che la reidentificazione è successiva rispetto alla valutazione d'impatto, che sarà stata già fatta senza averne tenuto conto, rimanendo quindi incapace di garantire l'effettività del nuovo diritto esposto agli attacchi dei BD.

Quanto detto non vuole essere un giudizio *in toto* negativo sulla valutazione, che pur presenta delle utilità anche se diverse da quella che qui assumiamo centrale: conservare un minimo indispensabile di privacy grazie a modalità di protezione inedite, adatte all'ambiente digitale, resistenti all'esposizione integrale dell'individuo e capaci di stare al passo con il mutare della tecnica.

La terza obiezione riguarda l'atteggiamento contraddittorio del legislatore europeo, che da un lato prova a capire il nuovo contesto tecnologico della privacy, nel momento in cui si avvicina al rischio; d'altro canto, continua a guardare al passato nel tenere presenti gli scopi «determinati, espliciti e legittimi» (art. 5, par. 1, lett. *b* Reg.) per i quali i dati vengono raccolti, trascurando che al contrario i fini connessi ai BD sono di regola ignoti o cangianti[16].

[16] O. Tene, J. Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, in *Stanford Law Review*, 2012, pp. 64 ss.

La quarta obiezione è l'«ossimoro della valutazione di impatto», perché per come è stata disegnata non si esclude che possa condurre al risultato opposto a quello sperato. Infatti, se l'analisi viene confortata anche dal *placet* del Garante, essa finisce per consegnare una semi-immunità giuridica al suo autore. Anche dunque il concerto dei Garanti, concepito come garanzia per gli interessati, potrebbe giocare contro di loro nel giudizio di responsabilità.

Invero, la norma non assume l'osservanza del dovere valutativo come esimente da responsabilità giuridica; ma se un significato le si vuole riconoscere, è quanto meno quello di aver ingenerato una ragionevole affidabilità circa la conformità della valutazione al diritto, salvo che il danneggiato provi che il danno trascurato si sarebbe potuto prevedere, valutazione a parte. Soffermiamo allora la nostra riflessione su quest'ultimo punto e costruiamo il ragionamento secondo i parametri pubblicistici della utilità sociale d'impresa (art. 41 Cost.). Quindi, omettiamo considerazioni sul titolo della colpa se *in vigilando* o in base ad altra *ratio*, perché terreno riservato alla scienza civilistica. Ma ricordiamo che un'attività pericolosa, quale la raccolta *omnibus* dei dati altrui, non può essere trattata alla stregua di una qualsivoglia attività d'impresa: si incorre in questo errore se si continua a ragionare in termini di responsabilità soggettiva per colpa o dolo. Se così si facesse, si negherebbe l'evidenza di un fatto e al tempo stesso si violerebbe una regola giuridica di base. L'evidenza è data dalla circostanza che la pericolosità di un'operazione può dipendere non solo dalla natura stessa dell'attività, ma anche dagli esiti rischiosi sulla collettività; mentre il diritto violato è nel trattare in modo diverso situazioni sostanzialmente simili, le analisi predittive e le attività pericolose *in re ipsa*, da equiordinare dunque anche nel regime di responsabilità.

Qui si sta sostenendo che la pericolosità delle analisi previsionali dovrebbe comportare la responsabilità dell'imprenditore per danni ai terzi coinvolti nella predizione, a prescindere dalla circostanza che l'imprenditore abbia fatto o meno quanto era in suo potere per evitare gli effetti dannosi.

Del resto, la dottrina civilista ha da tempo previsto forme speciali di responsabilità oggettiva per le attività rischiose, rientranti nella previsione generale dell'art. 2050 cc, qui l'evoluzione della tecnica deve portare a considerare pericolose operazioni un tempo inimmaginabili in ragione dell'oggetto inesistente: il dato da collezionare e modificare. L'aggregato collettivo è una massa grezza dei dati, un'entità dinamica, confusa e moltiplicabile all'infinito; il suo esito non è paragonabile alla conoscenza in origine stati-

ca, lineare e chiusa nella sua quantità, ora sostituita da un'informazione descrivibile in termini di flussi di *bit*. E le novità riguardano anche il modo di essere dell'evento di danno: esso consiste in analisi predittive che possono avere effetti pregiudizievoli per i soggetti coinvolti a prescindere dall'errore o dall'inesattezza della previsione. Si pensi a dati sanitari sensibili, raccolti anonimamente, in merito a una grave malattia inabilitante diffusa in una certa zona del paese, che quando furono collezionati servivano per accertare la responsabilità di industrie operanti nella zona. Successivamente venduti ad altri imprenditori, quei dati potrebbero servire per selezionare il personale e quindi per non assumere gli abitanti dei territori incriminati; queste persone subirebbero pertanto un danno indipendentemente da un errore di funzionamento dell'algoritmo, che invece aveva dato un'ottima prova di sé[17].

A nostro avviso questo ineliminabile fattore di incertezza, l'uso delegato e oscuro dei dati di terzi, dovrebbe comportare per chi li utilizza un aggravio di responsabilità, dalla quale questi non si dovrebbe poter sottrarre con la prova di aver fatto quanto era in suo potere, dovendo rispondere anche di ciò che è accaduto a prescindere da colpa o dolo. In questa nostra ricostruzione pesano il vincolo di solidarietà sociale, l'etica d'impresa, indifferentemente *off-line* o *on-line*, valori prevalenti sulla finalità lucrativa come richiesto dalla gerarchia costituzionale dei valori, ordinata a vantaggio del primo. Questa prospettiva pubblicistica induce a ipotizzare sul terreno civilistico una nuova forma di responsabilità oggettiva per rischio d'impresa, dove il mero fatto di trattare dati in forma massiva è rischio *in re ipsa* che fa scattare questo titolo speciale, derogatorio di responsabilità a carico del beneficiario dell'attività. Il fatto di aver reso la valutazione d'impatto secondo i dettati più o meno prescrittivi del Garante europeo serve al solo fine di evitare che il soggetto si esponga a ulteriori responsabilità rilevanti per il diritto amministrativo; lo esonera cioè da sanzioni amministrative verso il soggetto pubblico, ma lascia impregiudicata la sua responsabilità per lesione dei diritti delle persone, se lesione vi sia stata.

Se si considerasse l'assolvimento del dovere di valutazione titolo giustificativo di forme attenuate di responsabilità, si perverrebbe al risultato opposto a quello sperato, ossia all'«ossimoro da valutazione d'impatto». Invero, le attività pericolose finirebbero per godere di una semi-immunità, considerata la difficoltà per il danneggiato di provare che solo l'ulteriore sforzo di diligenza rispetto a quello reso con la valutazione avrebbe potuto evitare l'evento dannoso; e questo contrariamente alle attività ordinarie,

[17] Cfr. V. Mayer, S.K. Cukier, *Big Data*, cit., cap. 3.

che sono sottoposte alle severe regole generali della responsabilità per colpa, pur non generando pericoli diffusi per la collettività.

Anche sulla questione del titolo d'imputazione della responsabilità il Regolamento perde un'occasione: compiacente la materia che stava trattando, avrebbe potuto introdurre una nuova figura di responsabilità speciale da rischio d'impresa per fatto obiettivo, cioè indipendentemente dalla riferibilità psicologica, applicando la regola della corrispondenza biunivoca del lucro da rischio/aggravamento dell'*accountability* nel nuovo contesto dell'economia digitale. Invece ha preferito lasciare le cose come stanno, come se l'avvento di Internet non avesse modificato anche i meccanismi del diritto civile.

Infine, il carattere massivo della raccolta comporta altresì un nuovo modo di essere del danno, non circoscritto al singolo individuo, ma diffuso sulla collettività, coinvolta suo malgrado dall'analisi predittiva dell'algoritmo. A tal fine il legislatore europeo sarebbe potuto ritornare sulle *class action*, la cui spersonalizzazione del legittimato all'azione processuale ben si combina col concetto di danno diffuso, per meglio chiarire proprio le questioni lasciate aperte dai cattivi interventi legislativi su azioni di classi settoriali; ma anche in questo caso ha preferito lasciare la situazione così com'era.

Un'ultima obiezione riguarda la modalità di esternazione della valutazione[18], ma su questo punto c'è poco da dire perché il Regolamento tra l'opzione visibilità e la variante segretezza sceglie la seconda. Infatti, il suo art. 34, par. 9, prevede solo la facoltà, non già l'obbligo, per il titolare del trattamento di raccogliere le opinioni degli interessati «se del caso». Quindi, anche questo frammento di partecipazione, mal disegnato *ex lege* perché privo delle garanzie minime per gli interessati, è rimesso alla buona volontà dell'autore della valutazione, che per gentile concessione potrebbe accordare la partecipazione, degradata così da diritto ad aspettativa di mero fatto. Un ulteriore argomento esclude l'obbligo di pubblicazione: le Linee guida dei Garanti europei, prima ricordate, consigliano ai titolari del trattamento di pubblicare estratti della valutazione; *a contrario* il documento integrale è fuori dalla *best practice* indicata e comunque anche i meri estratti non sono oggetto della visibilità obbligatoria.

Quanto esposto nega che la conoscenza del funzionamento dell'algoritmo sia un diritto soggettivo, visto che già la sua premessa insuperabile, la conoscenza di questa valutazione, viene qui disattesa. Rispetto a questo

[18] Si veda: A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le Nuove Leggi Civili Commentate*, 1, 2017, pp. 156 ss.

dovere minimale il Regolamento è inadempiente perché decide di tenere i cittadini al buio digitale: nulla della valutazione, neanche il mero esito, è reso disponibile, neppure nelle forme selettive di pubblicità destinate alle sole categorie sociali coinvolte. Tutto rimane gelosamente custodito nei cassetti degli imprenditori, come se il farla (la pubblicità) fosse un fatto privato, al più da comunicare al Garante per essere rassicurati in merito alla legittimità della valutazione.

Noi invece riteniamo che la valutazione rappresenti il punto di avvio di quel processo cognitivo circolare che, partito in basso dai dati dei cittadini del *web*, ritorni come flusso di *bit* ai medesimi, le cui condotte sono state oggetto delle previsioni algoritmiche.

In sintesi, abbiamo rilevato un preoccupante silenzio del decisore europeo sulle questioni centrali: tipizzazione delle facoltà della nuova privacy, obbligo di visibilità dell'algoritmo funzionale alla sua giustiziabilità[19], apertura a *class action* ripensate e previsione di un nuovo titolo di responsabilità oggettiva per danni da BD. Ma il rimprovero più grave non attiene a ciò che il decisore politico non abbia fatto, quanto a quello che aveva annunciato di fare nelle promettenti dichiarazioni di principio, dietro le quali ha mascherato la conservazione dello *status quo*. Le sue buone intenzioni di passare dalla privacy da consenso del titolare a una da responsabilità dell'utilizzatore sono state sterilizzate nei *consideranda*, affidate quindi alla parte *soft* dell'atto normativo. A questo punto non rimane che sperare che possano essere raccolte e fatte proprie dal legislatore europeo di domani.

4. *I* Big Data: *una continuità discontinua con la* lex mercatoria

Il concetto di concorrenza è cambiato nel tempo: nasce come sinonimo di libero mercato, cioè come luogo dove persone, merci, capitali e prestazioni circolano indisturbatamente, al riparo, non solo dai protezionismi degli Stati, ma anche dai comportamenti abusivi delle imprese[20]. In seguito la *lex mercatoria* si lasciò alle spalle la visione atomistica a favore di una con-

[19] Questione in parte diversa, meritevole di una trattazione a parte, è la giustiziabilità di un atto autoritativo adottato in base ad algoritmo. La giustizia amministrativa ha avviato questo iter: si legga la convincente motivazione del Consiglio di Stato, sez. VI, 8 aprile 2019, n. 2270.

[20] Corte di Giustizia, *Grunding*, 56/64, p. 518, in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A61964CJ0056*, e Id., *Continental Can*, 6/72, in *https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A61972CJ0006.*

correnza che si compie incontrando anche le istanze dei consumatori. Una prova è rintracciabile nel rimedio previsto dal legislatore europeo degli impegni vincolanti[21]. Con essi la Commissione si interroga su quale possa essere la migliore soluzione per ripagare i consumatori danneggiati dalla condotta anticompetitiva (art. 9 Reg. CE 1/03): la mera *reductio in pristinum* o altra parimenti idonea a restituire efficienza competitiva al mercato.

La Commissione[22], per risolvere questa opzione, usa un parametro di giudizio inclusivo anche del benessere dei consumatori, senza però commettere l'errore opposto di sostenere una politica antitrust esclusivamente filoconsumeristica[23]. Un siffatto sbilanciamento unilaterale è stato evitato e corretto dilatando ancora una volta il concetto di protezione del mercato, che ora arriva a tenere insieme la difesa della domanda e dell'offerta con il *welfare* dei consumatori, beneficiari ultimi dell'equilibrio competitivo. In una espressione di sintesi: la concorrenza è diventata sinonimo del *well-being* collettivo, con l'avallo di una certa lettura della Corte di Giustizia[24].

Il Trattato di Lisbona ha contribuito a questo ampliamento di prospettiva aprendo il mercato alla nuova dimensione dello «sviluppo sostenibile dell'Europa, basato su una crescita economica equilibrata e sulla stabilità dei prezzi [...]. Essa promuove il progresso scientifico e tecnologico» (art. 2, co. 3, TUE).

Ma l'evoluzione della *lex mercatoria* è andata oltre Lisbona, perché l'erompere dell'economia digitale ha messo sotto tensione di nuovo la filosofia antitrust, costretta a rivedere ancora la sua identità. La nuova fase ci introduce in un nuovo scenario, dove l'economia confonde e mescola entità più eterogenee rispetto alle precedenti: competizione e *welfare* sociale, cosa diversa dal *well-being* dei consumatori. Questo significa che la *competition* deve concorrere all'equa distribuzione delle risorse – cioè rottura del monopolio dei dominanti del *web* sui BD – e servire alla causa della

[21] Cfr. par. 5 di questo saggio.

[22] Commissione Europea, *White Paper on modernization of the rules implementing Articles 81 and 82 of the EC Treaty*, in *J.O. C132/1,* 1999, in *Common market law Review. Executive Summary*, 5, 208, 1999, p. 8. In dottrina almeno: A. Jones, B. Surfrin, *EC competition law*, Oxford, Oxford University Press, 2010, pp. 43 ss.

[23] N. Kroes*, European Competition Policy – Delivering Better Markets and Better Choices, European consumer and competition day, London*, 15/9/2005, in *http://europa.eu/rapid/press-release_SPEECH-05-512_en.htm.*

[24] Si veda: Corte di Giustizia, *T-Mobile Netherlands, C-8/08*, in *https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A62008CJ0008*; Id., *GlaxoSmithKline, C-501/06 P, C-513/06 P, C-515/06 P e C-519/06 P*, in *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=ecli:ECLI:EU:C:2009:610.*

coesione territoriale. Stante l'universalità di Internet, quest'ultimo obiettivo potrebbe apparire a portata di mano; in realtà lo è a condizione che il decisore politico orienti il processo economico verso l'uguaglianza sostanziale. Se invece il mercato dovesse continuare a funzionare ripiegato su di sé, l'assenza di confini territoriali amplificherà i danni procurati alle parti deboli, un tempo circoscritti nei confini nazionali dell'economia *off-line*.

Questa tensione dell'economia all'uguaglianza sostanziale, cioè il suo agire come una leva per avvicinare i diseguali, comporta che si ripensi il modello dell'illecito antitrust. Nel senso che gli elementi di fatto della sua condotta *contra ius*, opportunamente non codificati dal legislatore col ricorso alla fattispecie aperta, integrabile da elementi *extra ordinem*[25], vanno rivisti alla luce dei BD e del loro fine ultimo. A nostro avviso, le masse dei dati dovrebbero essere al servizio della crescita individuale, dell'*equal access* a vantaggio degli altri operatori e del ritorno dei dati a chi li ha procurati *ab initio*. Chi sceglie il fine della conservazione dello *status quo*, cioè degli assetti di dominanza consolidati, non dovrà ripensare i paradigmi del diritto antitrust? Così come sono interpretati, aiutano i concorrenti esistenti sottraendoli alle pressioni dei nuovi entranti e quindi chiudono alla competizione effettiva, mantenendo un iniquo immobilismo.

Vediamo allora nei tratti essenziali[26] cosa diventerebbe l'abuso di posizione dominante, art. 102 TFUE[27] in un mercato *data driven*[28]. Assumiamo questa figura a emblema dell'illecito, pertanto le considerazioni seguenti varranno anche per le intese e le concentrazioni con gli adattamenti del caso. Ebbene, ricordiamo in breve che l'abuso si compone di un mercato di riferimento, una dominanza e un uso *unfair* di quest'ultima.

Poche parole per dire cosa è un'economia *data driven*: siamo in presenza di processi che hanno nell'accumulo crescente dei dati la loro benzina virtuale consistendo «in un complesso di attività che ruotano intorno alla produzione, all'uso e alla commercializzazione dei dati a mezzo di altri da-

[25] Volendo cfr.: G. De Minico, *Antitrust e Consob. Obiettivi e funzioni*, Padova, Cedam, 1997, cap. 1.

[26] Cfr. Commissione europea, *Antitrust procedures in abuse of dominance (Article 102 TFEU cases)*, in *http://ec.europa.eu/competition/antitrust/procedures_102_en.html.*

[27] Cfr. R. Wish-Baiely, *Competition law*, Oxford, Oxford University Press, 2018, capp. 17 e 18; R. Nazzini, *The foundations of European Union of Competition law: The objective and principles of article 102*, Oxford, Oxford University Press, 2011, *passim*.

[28] M.E. Stucke, A.P. Grunes, *Big data and competition policy*, Oxford, Oxford University Press, 2016, part. III, cap. 9.

ti»[29]. Ciò comporta che le imprese del settore tendenzialmente operino su due mercati collegati. Il primo si colloca a monte, dove beni e prestazioni digitali vengono offerti dietro una gratuità fittizia perché il consumatore paga con il valore dei suoi dati. Infatti, il rapporto contrattuale continua a essere sinallagmatico solo che il corrispettivo contro il servizio digitale non è il denaro, ma la cessione in blocco dei dati alla controparte.

Nel secondo mercato, quello a valle, si vendono tendenzialmente spazi pubblicitari in quanto l'impresa, grazie alla raccolta a strascico dei dati, vende questi spazi a prezzi più alti in ragione della quantità di dati affastellati sul mercato a monte. Alla fine del processo, i consumatori riceveranno pubblicità ritagliata sul proprio profilo, ricostruito grazie ai dati confluiti sul primo mercato. Non a caso, abbiamo detto che esiste un ordine tra il mercato gratuito e quello oneroso nel senso che il primo, solo in apparenza gratuito perché il dato sta in luogo del prezzo, alimenta l'appetibilità e quindi diventa la causa dell'onerosità di quello a valle, secondo quel perfetto circolo vizioso illustrato dagli economisti: più clic riceve il messaggio pubblicitario, più alto ne è il prezzo, e più voluminosa è la massa dei dati dell'imprenditore che domina le due piazze[30].

Ora proviamo a calare gli elementi indefiniti dell'abuso in questo nuovo scenario economico-tecnologico.

Il primo problema interesserà il metodo per individuare il mercato: non più il parametro classico della sostituibilità dei beni. È vero che vi si potrà ancora ricorrere per disegnare il mercato della raccolta pubblicitaria di Google o quello degli incontri virtuali di Facebook, come nell'esempio illustrato sopra, ma rimane fermo che i due mercati rimandano a una comune piazza virtuale, collocata sullo sfondo e alimentata dai dati; nonostante la Commissione si ostini a non considerarla tale perché non è identificabile secondo il criterio della fungibilità merceologica. Basterebbe riflettere che se preferiamo Google agli altri, non è per un suo specifico servizio – ad esempio quello di «Gmail», o di conservazione dei dati con «Google drive», oppure di incontri virtuali in «Google plus» – ma perché questo *Over the top*[31] è capace di offrire tutte le prestazioni e altre ancora nella

[29] M. Maggiolino, *I* Big data *e il diritto antitrust*, Milano, EGEA, 2018, nota 2, p. 2.

[30] A. Ezrachi, *Eu competition law goals and the digital economy. Report commissioned by BEUC*, 2018, in *https://www.beuc.eu/publications/beuc-x-2018-071_goals_of_eu_competition_law_and_digital_economy.pdf*, pp. 7-12.

[31] Autorità per le Garanzie nelle Comunicazioni, *Indagine conoscitiva concernente lo sviluppo delle piattaforme digitali e dei servizi di comunicazione elettronica. Allegato A alla delibera n. 165/16/CONS*, in *https://www.agcom.it/documents/10179/5054337/Allega-*

medesima unità spazio-temporale. Pertanto, chi fa parte della comunità di Google non è disposto a cambiarlo, a prescindere da come si comporti, in quanto al momento è l'unico operatore in grado di fornire una prestazione, pluriarticolata, sigillata in una scatola e portabile ovunque si vada. E qui ritorna il concetto d'insostituibilità, anche se in un'accezione globale perché è riferita all'intero pacchetto, non al singolo bene.

Le obiezioni pure pertinenti sollevate dagli economisti, le lasciamo appunto a loro. A noi giuristi basti sapere che è un fornitore *omnibus*, e per tale ragione incontestabile, perché fa incetta di dati da ogni suo cliente, cui offre su singoli segmenti i servizi più disparati, dalla posta alle recensioni dei luoghi con «Google maps». Per contro, dal lato dell'impresa, questo bagaglio in crescita esponenziale dei nostri dati è la benzina insostituibile, che tiene ben stretta perché su di essa ha fondato la sua dominanza.

Siamo giunti così al secondo elemento dell'abuso: il potere di mercato, certamente accertabile in base all'indizio del fatturato, ma vanno tenuti presente anche gli indici specifici connessi al *data driven*. Ad esempio, la dominanza di un'impresa del tipo in esame è costruita anche sulla circostanza che gli utenti la hanno preferita in ragione della scelta già fatta da altri: c.d. *lock-in*. Quindi, questo patto di sangue tra Google e i suoi clienti, che in economia si chiama «effetti diretti di rete», è un tratto incontestabile del suo potere di mercato.

Ultimo requisito per il perfezionamento della fattispecie di cui all'art. 102 TUE è l'abuso, perché ricordiamo che non si punisce la dominanza in sé ma il suo cattivo uso in danno di consumatori o concorrenti, come ricorre rispettivamente nelle due figure dell'abuso di sfruttamento e di esclusione. In estrema sintesi, il primo ricorre quando la condotta unilaterale dell'operatore si è risolta in comportamenti pregiudizievoli per i consumatori, che li subiscono senza andare a cercare altrove il medesimo servizio: tale sarebbe un aumento sensibile dei prezzi che lasci invariata la domanda. Il secondo abuso è riscontrabile in chi assume comportamenti dannosi per i concorrenti che nulla potranno fare per impedirli: si pensi all'imposizione di prezzi condizionati o di esclusive. In entrambi gli abusi la condotta contestata sarebbe quella propria di un monopolista, qui assunta da chi non lo è, ma si comporta come se lo fosse, perché può permettersi di prescindere dalle reazioni di consumatori e concorrenti.

Se proviamo a trasferire queste figure sui mercati *double sided* – cioè quelli che si articolano su due piazze, come illustrato prima – esse risul-

to+29-6-2016/9d7168c6-6205-47e7-a2d9-23cccdc1df59?version=1.0. D'ora in poi, per designare gli *Over the top*, useremo l'acronimo OTT.

teranno incomplete di un elemento essenziale al loro perfezionamento: l'aumento sensibile del prezzo. Ciò perché ad abuso commesso i beni continueranno a essere venduti a prezzo 0, e quindi mancherà un sintomo del cattivo uso del potere di mercato, salvo accettare la novità che la condotta illecita nell'ambiente digitale ha modalità alternative di esternazione rispetto a quelle dell'economia *off-line*. Si consideri quel dominante che, forte del suo pacchetto di dati, abbassa la *policy* di privacy senza subire una flessione nella domanda per il ricordato effetto di *lock-in* e per l'omogeneizzazione diffusa delle condizioni contrattuali. Siamo dinanzi a un abuso per sfruttamento, in quanto il dominante ha modificato unilateralmente le condizioni contrattuali, quali la *privacy policy*, pregiudicando i consumatori. Ora, se considerassimo questa *policy*, con tutte le difficoltà che ciò comporta, un elemento della disciplina del contratto, il degradarla inciderebbe sulla qualità della prestazione, ed ecco emergere un nuovo indizio di prepotenza nei confronti dei consumatori, benché la Commissione non lo veda.

L'impostazione qui suggerita rimanda a tre operazioni concettuali necessarie e preliminari.

a) Concepire il mercato come un luogo dove anche i diritti fondamentali possono essere violati con *vulnera* non meno gravi di quelli arrecati ai diritti economici dei consumatori.

b) Concepire il diritto, non più come una realtà divisibile in rigidi compartimenti stagni, incomunicabili tra loro, ma come composizione scomposta di sfere giuridiche che si possono mescolare – è accaduto per privacy e *competition* – e che si parlano, quando il terreno di gioco coinvolge più beni in modo vario e a diverso titolo[32].

c) Passare da una valutazione dell'illecito antitrust ancorata al solo indice quantitativo dell'aumento del prezzo, in quanto entità di facile rilevazione, a una più sofisticata basata sulla qualità del servizio, come tale inclusiva degli standard di privacy, di più ardua quantificazione[33].

Lo stato dell'arte è al momento molto deludente perché la Commissione con soluzione di continuità[34] si è sempre rifiutata di individuare una lesione all'art. 102 TFUE – *sub specie* di sfruttamento per aggressione alla privacy –

[32] F. Costa, C.O. Lynskey, *Family ties: the intersection between data protection and competition in EU law*, in *Common market law review*, 54, 11, 2017, pp. 12 ss.

[33] M.E. Stucke, A.P. Grunes, *Big data and competition policy*, cit., pp. 118-120.

[34] Commissione Europea, *Relazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Relazione sulla politica di concorrenza 2017, COM(2018) 482 final*, 18.6.2018, in *http://ec.europa.eu/competition/publications/annual_report/2017/part1_it.pdf.*

pur in presenza di un danno al mercato[35]. Noi non stiamo parlando di lesioni procurate alla sola privacy, ma di aggressioni che compromettono altresì la concorrenza. La Commissione si è trincerata dietro il rigido argomento della separazione delle competenze: a ciascuno il suo, la privacy al Garante europeo; la concorrenza a se medesima. In sintesi, un'operazione concentrativa non è mai stata annullata perché lesiva della privacy, se la stessa era conforme alla legislazione antitrust perché la Commissione ha sempre ritenuto le preoccupazioni sulla privacy «falling out of the aim of antitrust law», bensì «within the scope of the EC data protection rules»[36]. Questa è stata la giustificazione della Commissaria Vestager[37] quando le veniva richiesto di sanzionare come abusi i comportamenti di Google, ultima la sua condotta nell'offerta comparativa di pubblicità. La Commissione si è limitata a punire Google con forti sanzioni, lasciandolo perseverare indisturbatamente nella sua condotta abusiva, senza considerare peraltro che le pene pecuniarie, benché significative, non riescono ad avere una forza dissuasiva rispetto ai fatturati[38]. Questo è anche il caso di Facebook[39] per aver dichiarato il falso, quando acquistò WhatsApp, punito appunto per false dichiarazioni dalla Commissione, non per aver sottratto all'insaputa dei clienti di WhatsApp i loro dati telefonici, consolidando un già smisurato potere di mercato.

Il fatto che gli illeciti si ripetano nel tempo più o meno con le stesse modalità – si veda l'annunciata ulteriore fusione di Facebook con Instagram[40]

[35] *Contra* la Bundeskartellamt, *Bundeskartellamt prohibits Facebook from combining user data from different sources Background information on the Bundeskartellamt's Facebook proceeding*, February 2019, in *https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=5*.

[36] B. Bouyssière, D. Colgan, *Competition law, Big data and data protection – are Competition Authorities becoming jacks of all trades?*, in *https://www.lexology.com/library/detail.aspx?g=f9b02fe5-b8e1-4396-8efa-a24fffce9daf.*

[37] M. Vestager, *Competition in a Big data world*, 18 January 2016, in *https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-big-data-world_enin.*

[38] Commissione europea, *Caso AT.39740 Google search (Shopping)*, cfr. *IP/17/1784 del 27 giugno 2017*, in *http://europa.eu/rapid/press-release_IP-17-1784_it.htm*. Volendo cfr.: G. De Minico, *New horizons for the policymaker after the Commission's decision on Google?, 2017,* in *https://iaclaidc.wordpress.com/2017/08/27/new-horizons-for-the-policymaker-after-the-commissions-decision-on-google/.*

[39] Commissione europea, *Caso M.8228 – Facebook/WhatsApp, 18 maggio 2017*, in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017M8228(03)&from=LT*

[40] M. Isaac, *Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger*, in *NYT*, 26/01/2019, *https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html.*

– è la prova che questa interpretazione anacronistica del diritto antitrust non riesce a cogliere i veri comportamenti che strozzano il mercato, regalando ai dominanti l'impunità assoluta.

Questa nuova visione del diritto antitrust sostanziale richiederebbe altresì un accorto coinvolgimento nelle procedure antitrust anche del Garante privacy, da consultare obbligatoriamente ai fini dell'accertamento della lesione alla privacy, lasciando invece la valutazione del perfezionarsi o meno dell'illecito antitrust alla competenza della Commissione. Così la nostra impostazione riuscirebbe a combinare un nuovo modo di essere dell'illecito con un nuovo omaggio alla separazione dei poteri, che nelle società moderne è ordinata confusione delle attribuzioni piuttosto che rigida incomunicabilità delle competenze.

Abbiamo dunque individuato in capo alla Commissione un obbligo di presa in considerazione delle *privacy concerns* ai fini del perfezionamento dell'illecito antitrust, ma detto obbligo è deducibile anche *aliunde*, precisamente dall'articolo 8 della Carta dei Diritti. Consideriamo tre circostanze concorrenti: la vincolatività della Carta; la sua efficacia giuridica diretta verso tutti i soggetti istituzionali, dunque anche verso la Commissione; e, infine, l'accesso diretto dei cittadini alla Corte condizionato ai rigorosi requisiti della legittimazione ad agire. Da esse si evince che l'attivazione *ex officio* della Commissione è, non solo un dovere in ragione delle tre circostanze, ma anche la via più agevole per difendere un diritto, la privacy, altrimenti violato impunemente.

E a sviluppare fino in fondo questa impostazione giuridica si arriva a sostenere l'illegittimità di una delibera della Commissione di non luogo a procedere, nonostante la lesione della privacy, come di una delibera di imposizione di rimedi non tagliati anche sulla privacy. Nella specie le due delibere sarebbero illegittime per violazione della norma primaria, come tale su di esse prevalente, dell'art. 8 della Carta.

In conclusione, riteniamo che le misure sanzionatorie dovranno essere anche *privacy based*, non potendosi risolvere in meri ordini repressivi della sola condotta anticompetitiva: se i beni aggrediti sono due, anche la loro riparazione dovrà essere in grado di compensare entrambi i pregiudizi, ma questo lo vedremo in seguito.

5. *Gli impegni vincolanti al tempo dell'economia* data driven

Abbiamo preparato il terreno per ora passare a esaminare se e come i rimedi classici del diritto antitrust – ordine di cessazione, *desistat* e impegni vincolanti – possono cambiare quando i suoi destinatari operano in mercati digitali *data driven*.

Va tenuto conto del fatto che Internet non tollera i trasporti automatici di regole, cioè pensate per contesti materiali diversi e poi calatele dall'alto senza adattamenti. La specificità della rete va compresa e quindi protetta, in caso contrario si rischia di imporre camicie di forza, che ingabbiano il mercato senza correggerlo, con l'unico esito della fuga dei regolati verso piazze anarchiche.

Questa tipicità rispetto al mercato dei BD si chiama massa grezza di dati, tendenzialmente anonimi, generati dagli apporti *pro quota* di una collettività di uomini e imprese, poi utilizzati dai soli Giganti di Internet per i propri fini egoistici. In questo contesto di *data driven economy* svilupperemo il discorso sulle misure antitrust, in particolare sugli impegni[41].

In apertura abbiamo posto l'equazione tutela della concorrenza=protezione della privacy: essa significa che la difesa della privacy consumeristica è ora diventata uno *step* ineliminabile dell'*iter* antitrust; saltarlo procurerebbe una protezione dimidiata alla concorrenza, perché conseguita sacrificando le legittime aspettative di privacy dei consumatori, divenute elemento della qualità del servizio.

L'intreccio privacy/competizione, cioè la lesione del primo valore come sintomo di abuso di potere dominante, rende le misure tipiche antitrust *unreasonable* al caso nostro per due ragioni.

In primo luogo la tempestività, attributo dei processi economici in rete, richiede che le misure intervengano quanto prima, mentre attendere i lunghi tempi di un'istruttoria diretta ad accertare l'illecito compromette irreversibilmente i beni della concorrenza e della privacy. Da qui il ragionevole *favor* del legislatore europeo verso gli strumenti negoziali più rapidi a definirsi; almeno questa sarebbe l'aspettativa a fronte di un impegno il cui scopo è evitare l'accertamento definitivo dell'illecito con atto autoritativo. Accanto al fattore tempo un'altra considerazione li rende un buon rimedio per l'economia *data driven*; e qui la nostra attenzione si rivolge al secondo

[41] M. Botta, K. Wiedemann, *Eu competition law enforcement vis-à-vis explitative conducts in the data economy exploring the Terra incognita*, *Max Planck Institute for Innovation & Competition Research Paper No. 18-08*, 2018, pp. 1-89 (per gentile concessione degli Autori).

dei beni in campo, la privacy, che, se lesa, subisce un'aggressione senza ritorno. Pertanto, il classico ordine di cessare la condotta lesiva o il suo *desistat*, atti tipici di contrasto delle intese e degli abusi, non consentirebbero alla privacy di riacquistare la sua consistenza *ante delictum*, in quanto i dati, anche se restituiti ai rispettivi titolari, rimarrebbero violati per il semplice fatto di essere usciti dalla loro sfera giuridica. L'impossibilità di «turn the clock back» accorda un incontestabile vantaggio agli impegni rispetto alle sanzioni autoritative (artt. 101 e 102 TFUE).

Ora il terreno è pronto ad accogliere l'art. 9 del Regolamento CE 1/2003[42], in origine limitato agli impegni che regolano i traffici materiali, la cui estensione ai commerci *on-line* non incontra ragioni ostative. Piuttosto chiediamoci quale dovrà essere il contenuto prescrittivo dell'atto e quale il parametro valutativo della Commissione nel decidere se approvarlo o meno.

Solo poche parole per ricordare contenuto e finalità di un impegno[43]. Questo è una proposta di parte diretta a restituire l'efficienza competitiva al mercato al fine di evitare l'accertamento autoritativo del presunto illecito antitrust con quanto ne segue.

Pertanto, l'imprenditore dovrà offrire comportamenti capaci di sanare i due tipi abuso, prima esaminati: quello di sfruttamento e di esclusione. Precisamente, a fronte del primo, il rimedio consisterà nel rendere disponibili ai consumatori adeguati spazi per l'esercizio delle facoltà connesse alla loro privacy, violata dall'abuso.

Non sarebbe né possibile, né utile tipizzare in elenchi esaustivi la tipologia degli impegni in esame, in quanto il loro contenuto va modellato in vista della funzione: restituire al mercato, non necessariamente il medesimo *status quo ante*, bensì l'efficienza competitiva alterata dall'abuso. Ciò che conta è che il parametro valutativo dei costi e benefici, al quale la misura deve obbedire, rispetti la specificità dettata dal nuovo terreno di gioco. Ciò esclude ogni automatismo nel trasportare gli istituti dalla sede di origine a quella nuova, necessitando di adattamenti per il mutato contesto. Così il contenuto dell'impegno dovrà tener conto almeno di due circostanze: il tipo di lesione inferta alla privacy e la dimensione collettiva del diritto, stante la sua riferibilità non più al singolo, ma a diffuse collettività di utenti.

[42] *Regolamento (CE) b.1/2003 del Consiglio del 16 dicembre 2002 concernente l'applicazione delle regole di concorrenza di cui agli articoli 81 e 82 del Trattato*, in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32003R0001&from=IT.*

[43] N. Dunne, *Commitment decisions in Eu competition law*, in *Journal of competition law and economics*, 10, 2, 2014, pp. 399 ss.

La parte che seguirà di questo studio esamina casi accaduti o solo figurati, perché è l'approccio pragmatico della ricerca a richiederlo, in modo da offrire un modello prescrittivo capace di incontrare le preoccupazioni di privacy dei consumatori unitamente a quelle competitive.

a) Quanto al tipo di lesione rispetto all'abuso da sfruttamento, si ipotizza il caso di un'informativa così oscura per il consumatore da escludere la consapevolezza del suo consenso perché egli non ha inteso quali dati ha ceduto e a quali fini. Se questa asimmetria informativa dovesse integrare un'ipotesi di condotta *unfair*, perché l'abusante si è permesso un prospetto informativo inintelligibile, forte del fatto che i suoi clienti non si sarebbero rivolti a un altro *competitor* in assenza di migliori condizioni altrove e per il vincolo del *lock-in*, anche il *committement* dovrà fare i conti con tale opacità per porvi rimedio. Farebbe al caso nostro una proposta di obbligo di *disclosure* comprensibile in modo da restituire al consenso la dignità di atto volitivo libero e preso con cognizione di causa, considerato che l'intera disciplina europea ha rafforzato proprio questi requisiti, pur con qualche contraddizione.

Un'altra modalità di condotta abusiva si potrebbe risolvere nella lesione del diritto al libero consenso perché il consumatore, benché informato del peggioramento della *policy* di privacy, è rimasto fedele al fornitore originario del servizio digitale per omogeneità delle condizioni contrattuali. Quando la concorrenza non è basata sulla privacy, la persona perde ogni potere effettivo di contrattare e di reagire al degradamento, con la conseguenza che per lui il contratto digitale è un «take or leave». Se invece si ipotizzasse la concreta operatività del diritto al trasporto dei propri dati verso un'altra piattaforma *on-line*, il clima sarebbe diverso perché i concorrenti assumerebbero la privacy come elemento di differenziazione della prestazione gareggiando per offrire i migliori standard di privacy. Noi stiamo suggerendo un rimedio modellato sul paradigma dell'art. 20 del Reg. 2016/679, pur non richiedendone i relativi presupposti, perché in questa ipotesi il trasporto sarebbe la soluzione per rimediare a un illecito a doppia valenza. Si avvierebbe un moto virtuoso: il consenso ritornerebbe a essere libero, si spezzerebbe il monopolio degli OTT sui dati, contestati nella dominanza dai nuovi entranti, e quest'ultimi spingerebbero la privacy *to the top* per contendere clienti ai primi.

b) La seconda circostanza è connessa all'estensione a fisarmonica del diritto alla privacy, modulabile in ragione dell'età e dell'appartenenza del suo titolare a certe categorie socio-economiche. Recuperare questo modo di essere della privacy consentirà che gli impegni si articolino anche in mi-

sure *privacy-tuned*, cioè capaci di dilatarsi o restringersi a seconda di come il titolare voglia regolare il volume di tutela della sua riservatezza. Pertanto, se l'abuso ha danneggiato utenti poco propensi per ragioni economiche a difendere la privacy perché più inclini a barattarla contro la gratuità della prestazione *on-line*, il *commitment* potrà attenuare la misura di protezione, stante il fievole interesse dei suoi titolari, lasciando eventualmente più o meno inalterato il volume dei dati acquisiti dall'abusante. A opposta soluzione si perverrà se i danneggiati non vogliano cedere la privacy contro l'onerosità della prestazione, in tal caso si dovrà riconoscere la piena protezione del loro diritto con la conseguenza che il *commitment* dovrà prevedere la cessione dei dati al minimo indispensabile, vista la disponibilità dei titolari a pagare il servizio per mantenere integra la sfera personale.

Quanto detto pone un problema rilevante: le facoltà inerenti a un diritto fondamentale presentano uno *ius variandi* che dipende dalla capacità economica e di spesa del suo *dominus*. Ci rendiamo conto che il concetto di una privacy censitaria stride con i principi di democrazia, che nella sua accezione minima significa uguaglianza dei cittadini nella titolarità dei diritti dinanzi alla legge. Ma in questo caso non è negata l'equiordinazione nell'astratta titolarità del diritto, mantenuta uguale in capo a ciascuno, bensì è il suo concreto esercizio che viene modulato dalla volontà del titolare, che potrebbe dare precedenza a un bene diverso dalla sua sfera intima, ad esempio, alla piena gratuità della prestazione digitale.

Dagli esempi prima ricordati è emerso un contenuto dell'impegno definibile *case by case*, cioè in ragione della tipologia della lesione; questa è una caratteristica ricorrente nei provvedimenti impartiti d'imperio, ma assiste anche gli atti a genesi negoziale in quanto il fine comune è restituire al mercato rispettivamente la medesima o una diversa efficienza competitiva, il che richiede la *reasonables* dell'atto, cioè il suo essere non preconfezionato, bensì tagliato su misura alle concrete condizioni di mercato e sensibile col variare del tempo. Se allora consideriamo l'ipotesi in cui l'abusante abbia già ceduto i dati a terzi, qui un ritorno dei dati ai legittimi proprietari si rivelerà impraticabile, mentre il riferimento alla disciplina privacy potrà ancora una volta venire in nostro soccorso per definire il rimedio più adeguato. Si pensi allora a un contenuto che riconosca ai titolari la facoltà di esercitare i diritti, inizialmente azionabili verso l'originario detentore dei dati, anche nei confronti dei suoi aventi causa: così la rettifica, il controllo sulla sicurezza delle banche, la cancellazione dei dati o altre forme di tutela previste nel Reg. 2016/689 sarebbero opponibili ai nuovi utilizzatori dei dati.

Consideriamo ora la seconda figura di abuso, quello di sfruttamento che danneggia i terzi concorrenti, costringendoli a uscire dal mercato o impedendovi di entrare[44]. Esemplificativa è la condotta di quella impresa che ha emarginato i *competitors* dall'accedere ai dati comportandosi come se fosse la padrona incontrastata di questa massa informativa crescente nel tempo. Qui la condotta rimediale deve necessariamente prevedere la condivisione dell'*asset*, il solo rimedio idoneo a rimuove la barriera tecnologica all'entrata, pur consapevoli delle obiezioni che esso incontra perché disincentiverebbe gli investimenti, nonché per la difficoltà di valutare l'*asset* e di distinguere tra la massa dei dati quali mettere in comunione e quali no[45]. In questo contenuto di *sharing* aziendale si consuma il passaggio dal rimedio comportamentale, indicato prima, a quello strutturale della spartizione o co-uso dell'*asset*. Esso è perfettamente in linea con il Reg. 1/2003 (art. 7), che lo aveva contemplato e disciplinato a prescindere se la condivisione fosse imposta *ab initio* d'imperio o autoproposta dall'impresa e solo validata dalla Commissione. Quello che conta ai fini della legittimità dell'impegno è che la misura strutturale sia l'estrema *ratio* alla quale pervenire solo quando l'esame di ogni altra misura comportamentale risulti inefficace o più costosa, vista la maggiore intrusività di questo rimedio sull'autonomia aziendale rispetto a una misura comportamentale.

In questo caso ritroviamo gli estremi di un ragionamento svolto rispetto agli operatori di telecomunicazioni, *ex incumbent*, proprietari della rete ma anche fornitori dei servizi agli utenti finali. Il loro innato conflitto di interessi verso gli altri operatori privi di rete può comportare – a certe condizioni e in via residuale – che la rete sia a loro distratta per essere assegnata a un polo terzo, gestore neutrale. Questi tratterà in modo uguale le domande di accesso all'infrastruttura, non avendo nessun interesse nei traffici a valle; mentre l'ex proprietario della rete potrà in modo *fair* dedicarsi alla fornitura del servizio ai clienti finali.

Questa ipotesi comparativa che nella sua forma estrema conduce allo *split* della rete, mentre in quella intermedia alla sua separazione strutturale – con la conservazione della rete nelle mani del suo proprietario ordinario

[44] V. Kathuria, J.Globocnik, *Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy*, *Max Planck Institute for Innovation and Competition Research Paper No. 19-04.*

[45] M. Botta, K. Wiedemann, *Eu competition law enforcement vis-à-vis exploitative conducts in the data economy. Exploring the terra incognita, paper*, per gentile concessione degli Autori, 2019, *passim*.

nonché gestore del servizio di Telco[46] – presenta una differenza significativa dal caso dello *sharing* dei dati tra imprese *data driven*. Nel caso in esame i dati non sono mai stati dell'Over the Top, che li ha sì raccolti, aggregati e poi monetizzati per trarre profitti, ma non può vantare su di essi nessun titolo riservatario, che invece spetta alla collettività indifferenziata degli utenti per aver contribuito alla sua formazione. Ne consegue che la Commissione nel disporre la separazione dei dati dall'OTT dovrà usare meno cautela e discrezione di quella richiestale quando ordina la separazione della rete fissa di una Telco. Anzi in punto di diritto non riteniamo sia corretto parlare di separazione proprietaria, perché ci si separa solo da quello che già ci appartiene, e questo non è il caso degli OTT, meri detentori dei dati nell'interesse di noi utenti; sembra essere invece più coerente con il caso in esame il ricorso alla restituzione per indebita acquisizione. Pertanto, l'impegno dovrà disporre la libera fruibilità dell'asset-dati a qualunque operatore lo richieda; in tal modo si creerebbe quella circolarità diffusa dei dati utile a due obiettivi: incrementare la contendibilità dei mercati, nati come orti interclusi per l'esistenza di barriere tecnologiche all'ingresso (le masse di dati), e accrescere la democraticità del sistema economico, premessa alla democraticità dei processi politici.

Sembra evidente che qui si è definito il contenuto di un atto tipico della *lex mercatoria* prendendo a prestito il paradigma della privacy. Infatti, abbiamo tratto spunti dal Reg. 2016/679 per definire un contenuto non tipizzabile a priori. Bisogna però stare attenti a non commettere l'errore opposto a quello della Commissione, ostinata a dichiararsi incompetente nelle implicazioni delle violazioni antitrust sulla privacy, e cioè ritenere che ogni rimedio *privacy based* sia adatto *ipso iure* anche a riparare un'aggressione al mercato. Piuttosto sarà opportuno procedere *case by case*, senza valutazione legali tipiche o astratte presunzioni in modo da verificare se un certo rimedio diretto a proteggere la privacy sia anche idoneo a riparare il mercato aggredito. Nella *data economy* mentre un rimedio *privacy based* non soddisfa comunque le preoccupazioni della *competition*, invece una lesione della privacy è spesso sintomo anche di una violazione della legge del mercato, salvo accertare la ricorrenza degli altri elementi costitutivi dell'illecito antitrust.

Questa commistione tra privacy e *competition* – i cui beni rimangono distinti da un punto di vista ontologico, dei bisogni sottostanti, e quindi delle autorità competenti a proteggerli - non costituisce un errore valutati-

[46] Volendo G. De Minico, *Tecnica e diritti sociali nella* regulation *della banda larga*, in G. De Minico (a cura di), *Dalla tecnologia ai diritti*, Napoli, Jovene, 2010, pp. 3 ss.

vo, ma la naturale conseguenza di un diverso modo di intendere il diritto, non più ripartibile nella bipartizione classica pubblico/privato, né separabile in ragione dei beni da proteggere, mercato da privacy. I piani, un tempo separati, si sono ora mescolati; i beni, prima lontani e aggredibili da distinte condotte, sono esposti a lesioni progressive o sono tutelabili l'uno come conseguenza dell'altro; e le Autorità, un tempo incomunicabili, sono chiamate a parlare perché questo intreccio del diritto sostanziale impone un intreccio di poteri con proficua "confusione" di procedure.

Dinanzi a un illecito che è duplice violazione, alla concorrenza e alla privacy, anche il suo ritorno alla legalità dovrà soddisfare i due beni aggrediti; diversamente, ancora un lato dell'illecito rimarrebbe da riparare. La nostra lettura supera le rigide distinzioni e rompe le categorie concettuali del diritto, perché i BD hanno distrutto i vecchi schemi; allo studioso il compito di prenderne atto e provare a costruirne nuovi, modellabili sulla realtà quale è, non su come il giurista vorrebbe che fosse.

6. *E il cerchio si potrebbe chiudere a condizione di…*

Attratte privacy e *lex mercatoria* al valore dell'uguaglianza sostanziale, siamo giunti a questi esiti.

La privacy merita un trattamento orientato ai bisogni della collettività, il nuovo soggetto del diritto in aggiunta al singolo. Il passaggio dalla concezione atomistica a una collettiva della privacy[47] si giustifica per il beneficio atteso dalla frazione di collettività coinvolta dalle previsioni: partecipare al processo cognitivo formatosi con l'apporto di ciascuno.

Abbiamo conosciuto una privacy diversa da com'era agli inizi: ricca di nuove facoltà ma impoverita del consenso informato, sterilizzato per difetto di fini conoscibili *ex ante*. Questi poteri inediti, costruiti sull'irrobustimento dei doveri degli OTT, si articolano nella pretesa conoscitiva dell'algoritmo e nella sua confutabilità, nel caso comporti decisioni pregiudizievoli per la collettività, basate, non su comportamenti concretamente assunti, ma sul sospetto di probabili condotte. Questo spostare il fuoco dal consenso alla responsabilità degli OTT è la via moderna per incoraggiare l'inclusione di chi è rimasto indietro nei processi politico/economici; in ultima istanza ricentrare il gioco economico sui diritti fondamentali giova

[47] M. De Tullio, *Uguaglianza sostanziale e nuove dimensioni della partecipazione politica, Tesi in Diritti Umani. Teoria, storia e prassi – XXXI ciclo*, Napoli, 2018, cap. 3, par. 4.

alla democrazia, perché essa diventa sovranità effettiva solo se appartiene a un popolo consapevole nell'esercizio dei suoi diritti e libertà.

Quanto alla *lex mercatoria*, essa ha voltato pagina rispetto alla concorrenza funzionale al libero mercato, e si è lasciata dietro anche la competizione al servizio dei consumatori, firmando la "pace" con la solidarietà sociale. Questa lettura ha l'effetto di orientare il governo dei BD ai diritti e alla *lex mercatoria*.

Quanto ai primi, i dati raccolti dalle imprese meritano di essere trattati come un bene *open access*, disponibile anche alle imprese emarginate per consentire loro di contendere agli operatori dominanti il potere ingiustificatamente acquisito.

Mentre le figure d'illecito antitrust vanno interpretate in modo da incontrare le preoccupazioni di privacy e di altri diritti fondamentali insidiati, in coerenza col diritto dei Trattati che vincola la *lex mercatoria* alla coesione territoriale e allo sviluppo della persona, allontanandola dalle sirene dei nuovi protezionismi nazionali e delle lucratività solitarie.

Lasciare che la dinamica competitiva perseveri lungo questa china egoistica non giova neanche alla causa del libero mercato, perché alla lunga il benessere di pochi non può continuare a fondarsi sullo sfruttamento illimitato del disagio e dell'esclusione di molti. Soprattutto questa visione asfittica dei processi intrecciati, che si vogliono vedere distinti, rischia di soffocare l'ambizione politica europea anche sul piano del *common good*, della difesa prioritaria dei diritti sulle risorse, impedendo al circuito democratico di chiudersi. Perché esso prima di investire le istituzioni, deve rivoluzionare dal basso i processi economici e relazionali tra le genti d'Europa.

A queste condizioni potremo contare in avvenire su individui divenuti *cives* consapevoli dei loro diritti nel contesto digitale, e meno consumatori ignari di beni del mercato *on line.*

Big Data and the Weak Resistance of Legal Categories. The Case of Lex Mercatoria and Privacy

Big Data is the object of this legal discourse. The Author wonders whether and how this massive data collection disrupts the traditional legal categories and how to design new reasonable paradigms for Big Data. In particular, the *lex mercatoria* and privacy in the relationship with Big Data are taken into consideration. As for the *lex mercatoria*, the types of antitrust offenses if they maintain their constituent elements - markets and abusive of power - become empty skeletons because they will not be able to grasp the new dominances in the data drive markets. Instead, the Author proposes to make the *lex mercatoria* porous to the

changes of the technique and inclusive of the "abuses 4.0" committed by the Web Giants. Privacy has also been strained by the eruption of the phenomenon under consideration, which has rendered the original protection based on informed consent unnecessary. On the contrary, the essay opens up to unprecedented methods of protection: the visibility of algorithms within the limits of intelligibility and their submission to a strict judicial review for the predictive analyzes harmful to citizens. The argumentative path ends with a proposal for regulation, suitable of protecting the rights against the technical risks, but also capable of following up the tension of classical constitutionalism towards the substantial equality.

Keywords: Big data, Regulation, Lex Mercatoria, Privacy.

Giovanna De Minico, Professore ordinario di Diritto costituzionale, Università degli Studi Napoli Federico II, Via Antonio Gramsci 14, 00197 Roma, g.deminico@virgilio.it