LA RESPONSABILITÀ CIVILE DEGLI INTERNET SERVICE PROVIDER PER I MATERIALI CARICATI DAGLI UTENTI (CON QUALCHE CONSIDERAZIONE SUL RUOLO DI *GATEKEEPERS* DELLA COMUNICAZIONE) *

di LORENZO ALBERTINI

SOMMARIO: 1. Introduzione e delimitazione del tema. – 2. Il tipo di responsabilità. L'art. 2055 c.c. – 3. Responsabilità contrattuale o aquiliana? – 4. L'ambito soggettivo di applicazione. – 5. Si tratta di disciplina in negativo (esenzione da responsabilità), non affermativa di responsabilità. - 6) Le tre figure tipizzate e il problema della pretesa passività del provider. – 7. La pretesa passività e l'attuale modello di business delle piattaforme. – 8. Non necessità del requisito di passività (pur con qualche dubbio). – 9. Ancora ipotizzando di applicare il cons. 42 all'hosting provider. – 10. Alcune sentenze sul punto della pretesa necessità che si tratti di provider passivi. – 11. Sintesi del ragionamento sul tema della pretesa passività. – 12. Intermezzo su una recente e nota sentenza di Cassazione. – 13. Il provider di mero trasporto (art. 14 d. Lgs. 70/2003). L'inibitoria/injunction. – 14. Il caching provider (art. 15 d. Lgs. 70/2003). – 15. Cenni sul contenzioso intorno a queste prime figure di provider. – 16. L'hosting provider (art. 16 d. Lgs. 70/2003). Esatta attuazione delle norme europee? – 17. Esenzione da cosa? – 18. L'hosting provider può attendere fino al ricevimento di un ordine dell'autorità senza perdere il safe harbour? – 19. Posizione di garanzia? Primo arbitro tra interessi in conflitto, da dirimere con congruo bilanciamento. – 20. Inevitabilità del ruolo decisorio (e quindi censorio) su diritti soggettivi. Applicabilità dei diritti fondamentali anche verso enti privati come le piattaforme. – 21. (segue) recenti provvedimenti giurisdizionali italiani sul tema. – 22. Ancora sulla conoscenza richiesta dall'art. 16 c.1. – 23. Una ricostruzione della disciplina posta dall' art 16 c.1. – 24. L'art. 16 c.2. – 25. L'art. 16 c. 3. – 26. L'art. 17 c. 1: la non assoggettabilità a obbligo generale di sorveglianza o ricerca. 27. (segue) la sentenza Scarlet. Rilevanza dello stato della tecnologia, 28) Una recente opinione dell'AG presso la C.G. in causa C-18/18, Eva Glawischnig-Piesczek c. Facebook Ireland limited). - 29. L'inibitoria. Giurisprudenza europea in tema. – 30. L'inibitoria. Giurisprudenza italiana in tema. – 31. (segue:) l'ingiunzione c.d. dinamica. – 32. Sintesi sul divieto di istituire un obbligo generale di sorveglianza o ricerca ex art. 17 c. 1. Il caso europeo Eva Glawischnig-Piesczek c. Facebook Ireland limited, C-18/18. – 33. L'art. 17 c. 2. – 34. L'art. 17 c. 3. Cambiamenti in vista per la disciplina del safe harbour?

1. Introduzione e delimitazione del tema

In questo scritto esamino i principali profili di responsabilità civile degli internet provider[1] in relazione ad illeciti generati dalla messa on line di materiali da parte dei loro utenti. Intendo il concetto di <<responsabilità civile>> in senso ampio e cioè riferendolo non solo al rimedio risarcitorio, come spesso si legge, ma a tutte le conseguenze previste per l'illecito civile: tra cui soprattutto l'assoggettabilità a inibitoria/injunction (a prescindere dall'esistenza di una responsabilità risarcitoria)[2]. Questa può assumere anche un contenuto positivo appunto in termini di rimozione/disabilitazione[3], aspetto su cui giocano un ruolo decisivo le possibilità offerte dallo sviluppo tecnologico di un certo momento storico[4].

---

* Saggio in corso di pubblicazione in *www.medialaws.eu*, "Law and Media working paper series".

[1] Mi astengo dal precisare il concetto di *internet service provider*, a ciò bastando il requisito che sia coinvolto nella diffusione di contenuti caricati dagli utenti (si v. l'incipit degli artt. 12-13-14 dir. 2000/31 e norme corrispondenti nazionali; v. anche sotto). Tassonomia in Riordan J., *The liability of internet intermediaries*, Oxford University Press, 2016, p. 36 ss.(internet intermediaries) e 46 ss (offline intermediaries) nonché p. 387 ss sul concetto di *information society services,* cioè quelli cui si riferiscono i tre tipi di provider delineati dagli artt. 12-14 della dir. 2000/31.

[2] Per <responsabilità civile> si intende di solito la disciplina del risarcimento del danno (Mengoni L., voce *Responsabilità contrattuale (diritto vigente)*, in *Enc. dir.*, Milano, 1988, XXXIX, 1072; Bussani M., *L'illecito civile*, in *Tratt. dir. civ. del notar.* dir. da Perlingeri, Ed. Sc. Itl., 2020, 3 e 10). Se invece se ne amplia il significato, ad es. intendendola come «obbligo derivante dal torto» (G. Venezian, *Danno e risarcimento fuori dei contratti*, in *Opere giuridiche*, I, Roma, 1919, 55, cit. da C. Castronovo, *Responsabilità civile*, Milano, 2018, 3 nt. 1) o addirittura come <risposta solenne dell'ordinamento alla rottura di un equilibrio> (Maiorca C, voce *Responsabilità (teoria gen.)*, in *Enc. dir.*, Milano, 1988, XXXIV, 1004), allora comprenderà pure le misure reali, oltre che risarcitorie. Bisognerebbe poi capire quale fosse la tradizione comune europea sul concetto di responsabilità, vista la natura europea della norma. Scrive di *injunctive liability* Riordan J., *The liability of internet intermediaries*, cit., p. 14 e 19 ss.: l'a. precisa che, anche se astrattamente rimedio *non monetary*, tuttavia l'ottemperenza ad esso può comportare esborsi significativi (sub § 1.57). V. anche infra nota 468 e testo corrispondente.

[3] E' risaputo però che di solito ordina una condotta astensiva id est un *non facere*: cioè esprime un divieto (Stella M., *Inibitoria di opera in violazione del diritto di autore e copie in vendita su Amazon ed eBay*, in *Dir. di internet*, 2019/4, p.739, in nota a Trib. Torino, 25.07.2019 n. 3736, A.C. c. G.V.G.

[4] Sarebbero cinque le modalità per bloccarre l'accesso a siti web (*IP blocking, Blocking Based on Deep Packet Inspection, URL-Based Blocking, Platform Filtering, DNS-Based Blocking*) per Perel M., *Digital remedies*, in *Berkeley*

Stante la centralità dell'infrastruttura internet e dei servizi in esso presenti per qualunque attività umana o quasi, il tema, da un lato, è sempre più importante e, dall'altro, la sua disciplina giuridica non ha ancora raggiunto una soddisfacente sistemazione quanto a certezza del diritto[5].

Gli illeciti cagionabili dagli utenti tramite i servizi del provider possono essere di vario tipo ma soprattutto: violazione della riservatezza, violazione dell'onore o della reputazione, violazione della proprietà intellettuale (e qui particolarmente del diritto d'autore)[6].

---

technology law journal, vol. 35/1, 2020, 23 ss, riprendendo lo studio dell'I.SOC. *Perspectives on Internet Content Blocking: An Overview*, 24.03.2017. L'interessante saggio di Perel sulla fase esecutiva delle inibitorie, legata strettamente alla tecnologia, evidenzia la loro frequente genericità e dipendenza dalla (incontrollabile) discrezionalità delle piattaforme e offre qualche suggerimento alle Corti per ovviarvi: i) revisione successiva, ii) ricorrere ad esperti, iii) durate temporali limitate, iv) *contempt proceedings* per il caso di violazione, v) e molto interessante, aprire la partecipazione processual-esecutiva agli stakeholders affetti dagli eventuali errori di filtraggio (p. 42 ss). La centralità dell'elemento tecnologico (inconfutabile, del resto) è ricordata da Bellan A., *Piattaforme, obblighi di monitoraggio e risoluzione delle controversie online*, in *Il dir. ind*., 2020/2, p. 191; per l'a., tuttavia, questo non porterà alla soluzione automatica di tutti i conflitti né al superamento del divieto di sorveglianza/ricerca generale (p. 189).

[5] In parte non la raggiungerà mai: evolvendosi il panorama tecnologico, che amplierà l'offerta con servizi (magari solo in parte) innovativi, pure la loro disciplina risulterà via via inizialmente incerta. Del resto nella storia dell'esperienza umana i progressi tecnologici hanno sempre ampliato la sfera del pensiero anche astratto, per cui è inevitabile che pongano possibilità e questioni nuove (Schiavone A., *Progresso*, Laterza, 2020, 107-114, passim)..

[6] Tuttavia nell'ambito applicativo del d. lgs. 70/2003 non rientrano le <<questioni relative al diritto alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni di cui alla legge 31 dicembre 1996, n. 675, e al decreto legislativo 13 maggio 1998, n. 171, e successive modificazioni>> (art. 1 c. 2.b). Pertanto la responsabilità speciale da violazione della riservatezza, gravante su titolari e/o responsabili del trattamento dati (art. 82 reg. 2016/679, c.d. GDPR) dovrebbe prevalere sul *safe harbour*, posto dalla legge qui in esame. Il dubbio sorge dal fatto che la disposizione cit. del d. lgs. 70/2003 limita l'esclusione al <<trattamento dei dati personali nel settore delle telecomunicazioni>>: anche se nel caso di internet provider dovrebbe sempre trattarsi di "settore delle telecomunicazioni". Questo se l'internet provider costituisca titolare di trattamento, come succede se nelle clausole contrattuali, ove egli si riserva varie facoltà sui materiali caricati: così pure Bravo F., voce *Commercio elettronico*, *Enc. dir.*, *Annali*, V, 2012, § 24, 307 (che ipotizza pure il ruolo –improbabile, direi- di responsabile del trattamento di cui titolare sia l'utente/cliente). In senso contrario però potrebbe dirsi che la norma, quando considera «titolare del trattamento» <<*la persona fisica o giuridica, l'autorità*

Accettandosi la distinzione di base tra illecito contrattuale ed extracontrattuale, i casi normalmente considerati sono del secondo tipo (anche se nulla esclude che possano essere del primo tipo). Normalmente, infatti, la condotta lesiva tenuta non costituisce inadempimento di un'obbligazione o comunque di un dovere, sorto da una previa relazione fra le parti[7]: basta pensare ad una diffamazione o ad una contraffazione di diritto d'autore[8].

Se l'utente si rende responsabile di tali illeciti, si pone il dubbio di come qualificare giuridicamente la condotta dell'internet provider, dato che la pubblicazione del materiale è avvenuta tramite il provider stesso, in qualunque forma ammessa dalle modalità di funzionamento delle piattaforme[9].

pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali>> (art. 4 n. 7 del reg. 2016/679), intende chi di fatto procede a tali determinazioni, non chi semplicemente se ne riserva l'ipotetica possibilità (magari anche come licenziatario di più o meno specificate facoltà).

[7] Castronovo C., *Responsabilità civile*, Giuffrè, 2018, 502; Franzoni M., *Dei fatti illeciti. Art. 2043-2059*, in *Comm. cod. civ. cod. colleg. Scialoja Branca Galgano* a cura di De Nova, Zanichelli, 2020, 2 ed., 11 (conseguenza patologica di un preesistente obbligo inadempiuto). V. anche nota 37.

[8] Anche se l'interferenza con diritti altrui può avvenire violando non solo il divieto del *neminem laedere*, ma anche (è tema complesso quello del rapporto – cumulabilità- tra le due tutele) una regola pattizia: anche la seconda eventualità rientra nell'ambito coperto dalla dir. 2001/29 e dunque del diritto d'autore armonizzato (C.G., 18.12.2019, C-666/18, IT Development SAS c Free Mobile SAS).

[9] Esamina il concetto della *copyright publication* sul web Gerhardt D.R., *Copyright Publication on the Internet*, in *IDEA-The Law Review of the Franklin Pierce Center for Intellectual Property*, vol. 60/1, 2020, §§ IV-V. Per brevità, userò qui il termine "piattaforme" e "intermediari", da un lato, come sinonimi e, dall'altro, in senso ampio e cioè comprendendo pure i motori di ricerca, anche se a rigore potrebbero non essere ritenuti tali (vengono spesso distinti, anche da parte del legislatore: si v. spt. il reg. UE 2019/1150 del 20.06.2019 sull'equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online, ad es. conss. 2-4 lato utente e conss. 24-26 oppure art. 5 §§ 1-2 ad anche art. 7 §§ 1-2 lato venditori, per la distinzione tra servizi di intermediazione e motori di ricerca). Tuttavia anche i motori di ricerca forniscono un servizio di intermediazione: l'inserire un sito web nei risultati delle query, infatti, magari con un po' di *keyword advertising*, <<consente[ono] agli utenti commerciali di offrire beni o servizi ai consumatori, con l'obiettivo di facilitare l'avvio di transazioni dirette tra tali utenti commerciali e i consumatori>>, come recita l'art. 2 n. 2 reg. 1150/2019, cit. (conf. Gillespie T., *Custodians of the internet. Platforms, content moderation, and the hiddden decisions that shape social media*, Yale Un. Press, 2018, 40 e sua definizione di *platform* a p. 18-19). Ciò soprattutto qualora l'impresa scelga di essere presente non sui social ma solo col suo sito web (ipotesi tuttavia poco realistica, tranne per quelle di dimensioni minime), dato che sarà largamente

Questo termine (platform) è preferito dalle Big Tech per definire la propria attività, allo scopo di apparire neutrali per dare meno nell'occhio e operare con minori vincoli normativi[10] (anche se

condizionata dal posizionamento nei risultati delle ricerche (v. i cons. 24-26 del reg. 1150/2019; parla di "dipendenza" in tali casi Palmieri A., *Profili giuridici delle piattaforme digitali. La tutela degli utenti commerciali e dei titolari di siti web aziendali*, Giappichelli, 2019, 29-31). Del resto l'analisi economica considera anche i motori di ricerca come piattaforme, dato che anche essi mettono in contatto offerenti (di beni/servizi, ma anche di idee, a questo punto; *advertisers*, scrivono gli aa.) e consumatori (Katz M.-Sallet J., *Multisided Platforms and Antitrust Enforcement*, The Yale Law Journal, vo. 127-7, maggio 2018, 2143). Molti aa. comprendono nelle *digital platforms* pure i motori di ricerca: - Lao M., *No-Fault Digital Platform Monopolization*, *William&Mary Law Review*, (2020), vol. 61/3, pp. 775 ss, contestando la proposta di un approccio *no-fault* (rinnovato dalle c.d. *new Brandeis proposals*) circa la sec. 2 dello Sherman Act (*monopolization*) per allargare invece le categorie concettuali tradizionali (v. sub II.B le caratteristiche del mercato *network and lock-in effects* e p. 793 ss sulla proposta di scorporo avanzata nel 2019 dalla senatrice Elizabeth Warren, che curiosamente non comprende Microsoft, idea che torna di moda: Hiltzik M., *Mark Zuckerberg just made the case for breaking up Facebook*, in *Los Agenels Time*, 5 giugno 2020, ed. online e che non comporterebbe alcuna riduzione di concorrenzialità nella guerra tecnologica con la Cina, come osserva Sitaraman G., *Too Big to Prevail. The National Security Case for Breaking Up Big Tech*, *Foreign Affairs*, march/april 2020, foreignaffairs.com; sul tema v. l'interessante Cartwright M., *Internationalising state power through the internet: Google, Huawei and geopolitical struggle*, in *Internet policy review*, vol. 9/3, 2020, 1 ss.); - Katyal S.K.-Grinvald L.C., *Platform law and the brand enterprise*, in *Berkeley technology law journal*, vol. 32/3, 2018, 103; - Laidlaw E., *Mapping Current and Emerging Models of Intermediary Liability* (Calgary, June 15, 2019), leggibile in ssrn.com (li comprende negli intermediari, tra i quali rientrano le piattaforme quali intermediari particolarmente grandi, p. 8; v. schema delle categorie p. 12-13). Colloca invece la platform economy in una terza fase, dopo le internet companies di prima generazione (motori di ricerca: Google e Yahoo) e di seconda generazione (i primi marketplace: eBay, Amazon e Craiglist), detta terza generazione (web 3.0), <<in which technology is transforming the service economy, allowing greater access to offline exchanges for lower prices>> il saggio di Lobel O., *The Law of the Platform*, *Minnesota law review*, 2016, vol. 101, p. 95/6 (nella categoria più recente inserisce imprese tipo Airbnb, Uber, Lyft e in genere tutte quelle che operano quasi interametne via internet). Alcune piattaforme sono preferite da specifiche categorie professionali: ad es. Twitter e Instagram da parte di comici, artisti e influencer (Russ C., *Tweet takers & Instagram fakers: social media & copyright infringement*, Tulane J. tech. & intell. prop. 205 (2020), a p. 209) e notoriamente Linkedin dagli interessati a contatti professionali e/o per ricerca/offerta lavoro.

[10] Il termine "piattaforma" è infatti oggi largamente usato, perché sono gli stessi intermediari digitali a chiamarsi così, allo scopo di "*appear neutral, evade regulatory classification, or avoid the normative or professional standards that may come with a given domain*" (così il Report stilato da Caplan R., *Content or context moderation? Artisanal, community-reliant, and industrial approaches*, in *Data§Society*, 14.11.2018, p. 9 del file pdf); similmente Carroll E.c., *Platforms*

intendono al tempo stesso esercitare il potere decisionale assoluto sulla content moderation[11]). Possiamo accettare ad es. la definizione di piattaforme come "*large technology companies that have developed and maintain digital platforms that enable interaction between at least two different kinds of actors[;] who in the process come to host public information, organize access*

and the Fall of the Fourth Estate: Looking Beyond the First Amendment to Protect Watchdog Journalism, in *Maryland law review*, vol. 79/3, (2020), p. 558. Queste imprese curano accuratamente il *framing* con cui l'informazione pubblica le tratta e lo fanno <<*strategically, to position themselves both to pursue current and future profits, to strike a regulatory sweet spot between legislative protections that benefit them and obligations that do not, and to lay out a cultural imaginary within which their service makes sense*>> (Gillespie T., *The politics of 'platforms'*, in *New Media & Society*, 2010, vol. 12, 3, pp. 348, e poi analogamente in Gillespie T., *Custodians of the internet*, cit., 7). Del tutto simile la posizione di Napoli P.-Caplan R., *Why media companies insist they're not media companies, why they're wrong, and why it matters*, firstmonday.org, vol. 22/5, maggio 2017, che contestano analiticamente la prospettiva di presentarsi come imprese "tecnologiche", anziché come *media companies* (passim, ma, volendo, spt. i §§ *Underlying motivations* e *Why it matters*) e Napoli P., *Social media and the public interest. Media regulation in the disinformation age*, Columbia University Press, 2019, 5-16, che segnala anche la maggior attrattiva per gli investitori della catetgoria *technology company*, p. 15 (conf. Gillespie T., *Custodians of the internet*, cit., 7). Zuckerberg nelle audizioni al Senato USA del 2018 fu molto attento a non inserire la sua azienda in alcuna specifica categorie normativa <<*"I consider us to be a technology company" Zuckerberg said in response to a question as to whether Facebook was an advertising, publishing or telecommunications company, or perhaps a common carrier*>> (così Robert L. Kerr, *From Holmes to Zuckerberg: Keeping Marketplace-of-Ideas Theory Viable in the Age of Algorithms*, in *Communication Law and Policy*, 2019, vol. 24/4, 485; audizione che ha costituito <un fatto straordinario> per Flor E., *Il ruolo della comunità tra impresa e mercato*, in *Il Mulino*, 2020/4, p. 702). Serve però attenzione nel maneggiare il concetto di "piattaforma digitale", essendo talora usato con accezione diversa: v. ad es. in diritto pubblico la piattaforma per la notifica digitale alle pubbliche amministrazioni ex art. 1, c. 401, L. 27.12.2019 n. 160-art. 26 D.L. 76 del 16.07.2020 ovvero la "Piattaforma Digitale Nazionale Dati" ex art. 50 ter d. lgs. 07.03.2005 n. 82 novellato dal cit. D.L. 76 del 16.07.2020, art. 34. "Piattaforma" è termine con una lunga storia, inizialmente usato con significato religioso o politico: già nella Francia dell'*Ancien Regime* e nell'Inghilterra del 1500 (così Casilli A.A., *Schiavi del clic. Perché lavoriamo tutti per il nuovo capitalismo*, Feltrinelli, 2020 (orig.: 2019), p. 63/4). Distingue complessivamente cinque tipi di *platforms* Srnicek N., *Capitalismo digitale. Google, Facebook, Amazon e la nuova economia del web*, Luiss Un. Press, 2017 (or.: 2017), p. 47 ss e poi pp. 77-80: p. di advertising (Google, Facebook), p. cloud (AWS di Amazon, Salesforce), p. industriali (General Electric, Siemens: c.d. internet industriale che connette fornitori, produttore, consumatori etc.), p. prodotto (Spotify), p. lean (Uber, Airbnb)

[11] Paradosso rilevato da Suzor N.P., *Lawless. The secret rules that govern our digital lives*, Cambridge University Press, 2019, p. 16.

to it, create new formats for it, and control data about it[;] and who thereby influence incentive structures around investment in public communication (including news production)"[12].

In ogni caso, l'applicazione del safe harbour de quo richiede che si tratti di illecito derivante dalla diffusione di "informazioni": fattispecie che non ricorre ad es. quando derivi dalla fornitura di prodotti difettosi tramite la piattaforma (Amazon), nel qual caso a quest'ultima non spetta il safe harbour (lì il § 230 CDA)[13]. Fattispecie che ricorre invece quando la piattaforma abbia un minor coinvolgimento rispetto alla *res damnosa*, come succede se si limita ad anonimizzare la

[12] Così Carroll E.c., *Platforms and the Fall of the Fourth Estate: Looking Beyond the First Amendment to Protect Watchdog Journalism*, cit., p. 532, nota 19 (comprendente per l'a. Google, Apple e Facebook, chiamati *information gatekeepers*), e 547 ss sull'enorme importanza da esse raggiunta come mezzo di informazione. Si ivi l'esame del concetto di "*scale/scalable*", assai importante nell'economia delle piattaforme (op. ult. cit., p. 559 ss)

[13] Mi riferisco alla nota sentenza californiana dell'estate 2020, che ha ritenuto Amazon responsabile dei danni cagionati da scoppio di batteria per PC, venduta suo tramite da un produttore terza-parte (Court Of Appeal, Fourth Appellate District-division one-State Of California, *Angela Bolger c. Amazon*, 13 agosto 2020, DO75738). La sentenza ha appunto escluso che ricorra il caso di danno derivante da informazione fornita da un *content provider* terzo, derivando invece proprio dal prodotto fisico (e non ad es. da listino messo on line, come in un precedente giudiziario relativo a prodotti contraffatti commercializzati tramite eBay, invocato da Amazon ma respinto dalla Corte), nella cui distribuzione, poi, Amazon ha giocato un ruolo essenziale (*Discussion*, sub III, p. 41 ss., ove altri due casi citati). Anzi la sentenza è diventata nota (ed è importante) proprio per quest'ultimo aspetto: Amazon non può nascondersi dietro al fatto di non essere produttore né distributore, ma solo un fornitore di visibilità e di logistica. Essa invece va ritenuta responsabile perché attua (esige) un coinvolgimento complesso e quasi totale nel processo di vendita e distribuzione del prodotto: processo minuziosamente descritto in sentenza (*Discussion*, sub II, p. 17 ss.) e di cui sarà interessante vedere la qualificazione secondo il nostro sistema di responsabilità del produttore (soprattutto secondo il cod. consumo, artt. 114-116). Nemmeno ricorre la fattispecie delle "informazioni di terzi", quando un'impresa offre immagini di persone catturate illecitamente nei siti web (*screen scraping*) per offrire servizi di *facial recognitizion matching*: non solo non si tratta di informazioni di terzi (infatti il titolo azionato è l'illiceità della condotta dell'impresa, non delle fotografie raccolte) ma l'azione svolta nemmeno allega una funzione editoriale (così Vermont Superior Court-Chittenden unit-civil division, 10.09.2020, docket 226-3-20 Cncv, *State of Vermont v. Clearview AI inc*, rigettando la difesa del § 230 CDA.: si trattava di azione promossa dallo Stato per vioalazione del Vermont Consumer Protection Act e del Vermont's Fraudulent Acquisition of Data law).

navigazione nel dark web (TOR)[14] (né vedrei alcun motivo - letterale o teleologico- per escludere l'applicazione dei safe harbour alle condotte tenute sul web non indicizzato dai consueti motori di ricerca[15]) o se si limita a fare da bacheca per annunci di vendita di oggetti pericolosi[16].

Non considererò dunque i casi, in cui il provider stesso sia responsabile o corresponsabile per aver creato e/o consapevolmente diffuso il materiale illecito: penso non solo al caso di diffusione di materiale proprio, ma anche alla funzione c.d. *Auto complete*, che i motori di ricerca solitamente offrono, suggerendo, dopo le prime parole digitate, altre parole che – secondo le sue rilevazioni algoritmiche- vengono spesso digitate in abbinamento ad esse[17]. Considererò solo i casi in cui egli sia estraneo a ciò: casi nei quali, dunque, il dovere da lui violato sia

[14] Corte distrettuale dello Utah, Seaver c. The TOR Project e altri, 20.05.2019, case n. 2:18-cv-712-DB (azione svolta dai genitori di un ragazzo rimasto ucciso da droghe acquistate sul dark web).

[15] Si porrebbero semmai eventuali problemi di determinazione del danno per fattispecie diffamatorie o di violazione di proprietà intellettuale.

[16] Si veda Corte Suprema del Wisconsin 30.04.2019, caso n. 2017AP344, *Yasmeen Daniel c. Armslist ed altri*, riferita infra.

[17] Secondo il Bundesgerichtshof tedesco (14.05.2013, VI ZR 269/12, leggibile in *Dir. informazione informatica*, 2013, 541 ss. nota Giannone Codiglione G., *Funzione autocomplete e neutralità del prestatore di servizi*), l'abbinameno tra nome dell'attore e qualifiche offensive, proposte con l'*Auto complete*, per quanto frutto di rilevazioni da ricerche degli utenti, è imputabile al software di Google e dunque costituisce materiale proprio di questi, anziché dei predetti altri utenti. Non ha dunque applicato il safe harbour, ma la disciplina generale, ritenendo però che, secondo un giusto equilibrio tra i contrapposti interessi, il dovere di controllo a carico del motore di ricerca sorga solo quando venga a conoscenza della violazione del diritto. Nello stesso senso Trib. Milano 25.05.2013 ord., sez. I, est. Miccichè, in De Jure, relativo ad *Autocomplete* e a *Ricerche Correlate* di Google, reclamo cautelare; è però inesatta la motivazione, laddove si basa sul fatto che ciò farebbe venr meno la *passività* di Google: la distinzione provider attivi/passivi, infatti, ha senso per i materiali caricati dagli utenti, non quando si tratta di condotta riconducibile solamente al provider. Il punto non è semplice, dato che anche l'elenco dei risultati, proposto senza l'*Auto complete*, è frutto solamente degli algoritmi di Google. La differenza tra i due casi allora va ravvisata nel fatto che, mentre nei risultati con Autocomplete è solo l'abbinamento proposto da Google (tramite tale servizio accessorio) ad essere offensivo (e non le ricerche degli altri utenti, che non sapevano o volevano che queste venissero riproposte in modo algoritmicamente massivo a terzi), invece nei risultati senza Autocomplete il ruolo di Google è assai meno significativo, dato che le violazioni sono apportate in prima battuta dai siti internet, cui puntano i link risultati dalla ricerca (secondo le sue imperscrutabili istruzioni algoritmiche) tramite il motore di ricerca.

quello di filtraggio/rimozione dei materiali medesimi.

Nemmeno considererò il caso dei post temporanei (c.d. storie, stories), anziché permanenti, oggi assai diffusi su certe piattaforme (ad es. Snapchat, Instagram e –pur se poco conosciuto- Facebook). Si tratta di violazioni allo stato sostanzialmente non perseguibili, data la loro brevissima durata (di solito ventiquattro ore): la quale può però disturbare molto i titolari del diritto d'autore, ad es. quando siano caricati da influencer con larghissimo seguito oppure siano raccolti in compilation[18].

2. Il tipo di responsabilità. L'art. 2055 c.c.

Secondo lo scenario ipotizzabile, l'utente in un primo momento carica i materiali illeciti e il provider in un secondo momento (resta da capire esattamente quando: il punto è centrale) omette di rimuoverli. Per la precisione si dovrebbe dire che il dovere è duplice, dovendosi distinguere tra il dovere di rimuovere i materiali già caricati e (eventualmente) quello di disabilitare l'accesso per prevenire futuri caricamenti: questa distinzione, del resto, risulta in modo netto dalla normativa.

La disabilitazione dell'accesso potrebbe generare qualche problema contrattuale, poiché l'utente, che ha caricato i materiali (o forse il titolare dell'utenza dalla quale il caricamento è avvenuto), in mancanza di pattuizione specifica, potrebbe ravvisare in ciò un inadempimento al contratto: ma questo comunque riguarda il rapporto provider/utente e non il rapporto tra provider e terzo leso (che di seguito verrà per brevità indicato anche come "il soggetto leso").

In breve la responsabilità del provider per l'illecito de quo è una responsabilità omissiva, dal momento che non ha tenuto la condotta doverosa. In particolare, secondo una approfondita (e nelle sue linee essenziali condivisibile) ricerca, la condotta del provider si innesta su quella del suo utente, che la precede nel tempo. Il rapporto tra le due condotte è quello di un concorso sopravvenuto (da parte del provider) nel medesimo illecito: precisamente, all'iniziale comportamento commissivo del solo

[18] Sperling D., *Oh Snap! Time to Face Temporary Copyright Infringement*, in 3 *Georgetown Law Technology Review*, 2018, 82 ss., che scrive di *regulation gap*. Secondo l'a., le piattaforme potrebbero introdurre dei filtri atti ad operare nel ristrettissimo termine indicato, ma per qualche motivo non lo fanno (almeno per quanto è dato sapere: p. 111).

utente, segue quello omissivo da parte del provider[19]. Scrivo "segue" perché, pur essendo il provider di fatto presente sin dall'inizio, tuttavia, in linea di massima (ma si vedrà poi qualche precisazione sul punto) nulla gli può essere inizialmente addebitato: egli infatti non ha responsabilità di controllo sui contenuti del tipo della responsabilità editoriale (artt.57 e 57 bis c. pen. e art. 11 legge 08.02.1948 n,. 47)[20], come era stato invece deciso nei primi interventi giurisprudenziali[21]. Non potendoglisi

[19] Bocchini R., *La responsabilità civile degli intermediari del commercio elettronico. Contributo allo studio dell'illecito plurisoggttivo permanente*, ESI, 2003. cap. secondo, spt. 197 ss. Nel cap. terzo è sviluppata la tesi per cui si tratta di illecito permanente ed unitario, a partecipazione postuma (p. 223) , le cui conseguenze applicative principali riguardano il dies a quo del termine prescrizionale (p. 224 ss) e l'applicabilità dell'art. 2055 (p. 228/9). Su quest'ultimo punto si può però osservare che l'art. 2055 si applica anche a condotte reciprocamente autonome, qualora cagionino il <<medesimo fatto dannoso>> inteso come evento di danno (cioè dal punto di vista del daneggiato): Gnani A., *la responsabilità solidale. Art. 2055*, in *Il Cod. Civ. Comm.* dir. da Busnelli, Giuffrèè, 2005, p. 133 ss e 143 ss.

[20] L'equiparazione ad un editore è forse il mggior rischio per Facebook, secondo l'opinionista del *Financial Times* G. Rachman, *Facebook is the world's most powerful adolescent*, www.ft.com, 21.10.2019. Questo è probabilmente il tema centrale oggi sui social media: visto che di fatto si sono sostituiti alla stampa del mondo analogico come mezzo di circolazione delle informazioni, possono respingerne la relativa disciplina solo perché i post non sono previamente visionati e autorizzati? O per lo meno non lo sono individualmente, dato che il flusso di informazioni è ritagliato (*customized*) sull'utente in base ai moltissimi criteri implementati nell'algoritmo. Non vede distinzioni sostanziali (almeno a livello di influenza sulla popolazione) tra i tradizionali fornitori di contenuti (Disney, il television network HBO, Fox News o il Neww York times) e Facebook e Youtube, il saggio di Cohen J.E., *Between truth and power. The legal constructions of informational capitalism*, Oxford University Press, 2019, 99 ss; per questa a. (e per molti altri aa., per vero) ha avuto fondamentale importanza per il business delle piattaforme la norma del Buon Samaritano che il Communications Decency Act del 1996 ha inserito nel 47 US Code il § 230 *Protection for private blocking and screening of offensive material*, (v. il testo in law.cornell.edu) (d'ora in poi semplicemente: § 230 CDA) Secondo quest'ultima disciplina, in breve, i provider (o gli utilizzatori dei loro servizi) non saranno trattati come editori nè risponderanno per rimozione/disabilitazione eseguita in buona fede o per aver fornito strumenti a questo scopo a content provider (§ 230.c.1-2). La regola di irresponsabilità in linea di principio dei provider, posta dal diritto UE, prende le mosse dalla constatazione che l'hosting provider non è accostabile analogicamente all'editore, secondo Giannone Codiglione G., *Internet e tutele di diritto civile*, Giappichelli, 2020, 90-91.

[21] V. Pasquino T., *Servizi telematici e criteri di responsabilità*, Giuffrè, 2003, 242 ss; Stefanelli F., *La responsabilità dell'internet provider*, Graus Editore, 2018, 19 ss. Ipotizza la responsabilità editoriale Allegri M.R., *Ubi social, ibi ius. Fondamenti costituzionali dei social network e profili giuridici della*

quindi addebitare una violazione ab initio, gli si può però addebitare una violazione successiva, quando, pur potendo e dovendo, non ha rimosso i materiali illeciti (un'omissione, come si diceva).

Bisogna allora capire quale sia il momento, in cui sorge questo dovere di rimozione. Fino ad allora, come detto, nulla gli può essere addebitato, sicchè l'illecito è ancora monosoggettivo.

---

responsabilità dei provider, Franco Angeli, 2018 (open access), 131 ss. La questione però è di complessa soluzione, alla luce sia della totale dipendenza dei newsfeed e dei risultati delle queries dalla progettazione algoritmica, sia della loro non accessibilità e conoscibilità: per cui non è affatto escluso che gli effetti giuridici sfavorevoli (o alcuni di essi), relativi agli editori, vengano estesi (in via pretoria e/o anche legislativa) alle piattaforme. Le considera degli editori Bell E., *The unintentional press. How technology companies fail as publishers*, in Bollinger L.C.-Stone G.R., *The free speech century*, Oxford University Press, 2019, 235 ss; analogamente attribuisce loro la tutela del Primo Emendamento Goldman E., *Of Course the First Amendment Protects Google and Facebook (and It's Not a Close Question)*, in Pozen D.E. (a cura di) *The perilous public square. Structural threats to free expression today*, Columbia Un. Press, 2020, 146 ss., dato che fanno proprio ciò che per *Zeran v. American On Line* (notissima sentenza del 1997) è tipico dell'editore (<"deciding whether to publish, withdraw, postpone or alter content.">, replicando al saggio di Whitney cit. subito sotto), anche se è a fini difensivi è più utile invocare il § 230 CDA che il Primo Emendamento (Goldman E., *Why Section 230 Is Better Than the First Amendment*, 95 Notre Dame L. Rev. Online 33 (2019), 36-39 e 44-46). Critica invece *l'editorial analogy* Whitney H., *Search Engines, Social Media, and the Editorial Analogy*, in Pozen D.E. (a cura di) *The perilous public square. Structural threats to free expression today*, cit., 115 ss e spt. 121-134, passim, con riferimento a *Trending News* di Facebook e alla funzione *autocomplete* nel motore di ricerca di Google: l'a. così nega che l'applicazione dei relativi algoritmi costituisca *speech* protetto dal Primo Emendamento (anche perchè così è percepito dal pubblico: pp. 125-127), pur continuando le due Tech companies –contraddittoriamente, forse- da un lato ad invocarlo ma dall'altro ad escludere con veemenza la loro equiparabilità ai media tradizionali (v. nota prec.), dichiarando di limitarsi a diffondere opinioni degli utenti. Rileva analoga contraddizione nella condotta delle piattaforme Conroy A., *The First Amendment's Role on the Internet Governed by Private Actors: Disclosure Requirements as the "Best of Disinfectants"*, in 27 *Geo. Mason L. Rev* 381 (2020), 390/1, quando pretendono, da un lato, di poter censurare i post degli utenti, invocando il Primo emendamento quali *content curator*, e, dall'altro, però, di non risponderne quando siano illeciti ("platforms want to have their cake and eat it too"). Se rilevino, ai fini della responsabilità editoriale, simili dichiarazioni di intenti delle società tecnologiche oppure la loro concreta gestione dei documenti caricati dagli utenti (cioè se si debba far prevalere un criterio soggettivo od oggettivo), è questione solo apparentemente difficile (essendo senz'altro preferibile la seconda alternativa): piuttosto, la reale difficoltà consiste nel capire se la mera organizzazione, selezione, promozione etc. dei materiali altrui costituisca attività editoriale (in questo saggio si esclude che faccia perdere il safe harbour ex dir. 2000/31).

Dopo quel momento, invece, l'illecito diventa plurisoggettivo, anche se con due modalità diverse: una commissiva (la prima nel tempo, dell'utente), l'altra omissiva (quella successiva, del provider). La fattispecie plurisoggettiva sarà governata dall'articolo 2055 c.c. sia perché altre norme non ci sono, sia perché qualunque violazione, se concorre causalmente a produrre il medesimo evento di danno, rientra nell'ambito applicativo della norma stessa[22].

Nel diritto d'autore, accenna a questa fattispecie di responsabilità l'Avvocato Generale (di seguito: AG) Szpunar in *Ziggo v. The Pirate Bay (TPB)*, secondo cui quest'ultima piattaforma (gestore di rete peer-to-peer) realizza una comunicazione al pubblico dal momento, in cui viene a sapere dell'illiceità dei file la cui condivisione essa agevola[23]. L'AG precisa poi che, se invece si ritiene assente la responsabilità primaria di TPB, il giudizio su una eventuale responsabilità secondaria (o indiretta) è di competenza degli ordinamenti statali, non essendo stata armonizzata[24]. L'opinione è di dubbia esattezza, dato che la dir. 2001/29, invocata dall'AG per la sua prevalenza sulla dir. 2004/48[25], parla genericamente di "violazioni" (art. 7 e art. 8): concetto la cui ricostruzione dunque può comprendere anche il profilo soggettivo e che spetterà alla C.G. A meno di distinguere tra una responsabilità primaria e una secondaria (meramente agevolativa), in tal modo escludendo la seconda dall'armonizzazione europea: solo che quest'ultima verrebbe gravemente pregiudicata se ogni questione sull'agevolazione (responsabilità secondaria o indiretta) fosse liberamente regolabile dai singoli Stati (per non dire dell'incertezza che regnerebbe sulla stessa distinzione tra responsabilità primaria e secondaria, diversamente disciplinata

[22] Per aversi concorso ex art. 2055 basta infatti l'apporto causale alla produzione del medesimo fatto, come emerge dalla disposizione, e sulla base dei criteri di imputazione valevoli per le fattispecie monosoggettive, (v. Gnani A., *La responsabilità solidale. Art. 2055*, in F.D. Busnelli (dir. da), *Il cod. civ. Comm.*, Milano, 2055, p. 17-21).

[23] Conclusioni AG Szpunar 08.02.2017, Ziggo – The Pirate Bay, C-610/15, §§ 51-53.

[24] Al § 65.

[25] Al § 56

negli Stati UE)[26].

Ciò pare anzi confermato dal § 3 dell'art. 8 dir. 2001/29, invocato dal cit. § 56 delle Conclusioni dell'AG: che impone agli Stati di prevedere un'inibitoria contro gli "intermediari", i cui servizi sono utilizzati per la violazione. Da un lato, tale disposizione non necessariamente porta a contrapporre autori della violazione ad intermediari e cioè non impedisce di ritenere che i secondi possano rientrare tra i primi; dall'altro lato, anche ritenendo il contrario, il concetto di "intermediario", facendo parte del diritto UE, va interpretato dalla C.G. (è di portata così ampia che può anche comprendere TPB). La complessità del tema, però, merita specifico esame, qui non possibile.

Un profilo importante, a proposito dell'articolo 2055, è quello soggettivo, nel senso che non è chiaro se sia o meno richiesta anche la consapevolezza di compartecipare alla produzione di un danno ingiusto. Si potrebbe rispondere di si, dato che in generale ognuno deve rispondere di ciò che sa o poteva sapere, non di ciò che non poteva sapere: se il concorso ex art. 2055 costituisce un aggravio rispetto alla scelta della responsabilità (parziaria) monosoggettiva[27], il concorrente deve poter sapere del rischio di concorso (cioè di essere concorrente). Sembrano però più persuasive le ragioni addotte da chi nega che questo

[26] Che in effetti pare poco giustificata sia in astratto sia in base al nostro art. 2055 cc. Curiosamente proprio l'AG nelle prime battute delle sue Conclusioni affronta il punto. Riferisce che, secondo la Commissioni ed altri Stati intervenuti in causa, la questione di responsabilità sub iudice competerebbe solo ai singoli Stati: opinione respinta dall'AG, dato che <<*un siffatto approccio farebbe tuttavia dipendere tale responsabilità e, quindi, la portata dei diritti appartenenti ai titolari, dalle soluzioni, molto diverse, accolte nei vari ordinamenti giuridici nazionali. Orbene, tale circostanza comprometterebbe l'obiettivo della normativa dell'Unione nell'ambito del diritto d'autore, relativamente copiosa, che consiste proprio nell'armonizzare la portata dei diritti di cui godono gli autori e gli altri titolari nel mercato unico*>>, § 3. La presa di posizione sembra riguardare una fase per così dire preliminare di ammissibilità della questione: per passare poi, nel merito, a distinguere tra responsabilità primaria e secondaria (oppure diretta ed indiretta), riservando al diritto UE solo la prima, come accennato nel testo.

[27] Quando ad es. le conseguenze della condotta singola sarebbero state minori, rispetto a quelle derivate dal concorso: il riequilibrio, dato dall'azione di regresso, che per la dottrina permette di escludere l'incostituzionalità dell'equiparazione di tutti i contributi causali, grandi o piccoli e dunque anche minimi (c.d. peripheral tortfeasor: Gnani A., *La responsabilità solidale. Art. 2055*, cit., p. 14 ss.), non è però completo, dato che dover agire in giudizio è onere assai pesante per la maggior parte delle persone.

elemento soggettivo sia richiesto[28]: ma il punto qui non è importante, dato che il provider, da quando sorge il suo dovere di attivarsi, sa per definizione della condotta del suo utente (se si accetta questo punto fermo; e d'altro canto pure l'utente per definizione sa di poter divulgare il suo post solo tramite la piattaforma).

La dottrina predetta ha evidenziato che, sia dal tenore letterale sia dalle interpretazioni fino ad oggi succedutesi, l'articolo 2055 è stato tradizionalmente studiato ed applicato a condotte contestuali; tuttavia l'a. ritiene di estenderne l'ambito applicativo anche al caso nostro, in cui la condotta imputabile di un soggetto è successiva a quella dell'altro[29]. In effetti la norma dice semplicemente di <<fatto dannoso imputabile a più

[28] Secondo la tesi estensiva, per il ricorrere della solidarietà basta che sia unico l'evento dannoso (cioè l'interesse leso): v. l'approfondita analisi di Gnani A., *La responsabilità solidale. Art. 2055*, cit., 133-171 (spec. 133-134 e 163-165; e ciò anche se le condotte e le loro conseguenze sono separabili: 161-162). Questo a. segnala che secondo i *Principles of european tort law* (http://www.egtl.org, anche in italiano, art. 3:104, co. 2), <<un'attività successiva è presa in considerazione se ha comportato danni ulteriori o più gravi>>: ed è il nostro caso, in cui la mancata rimozione comporta non un evento distinto dall'hosting del file dell'utente, bensì il protrarsi dell'hosting stesso e dunque l'aumento di gravità dell'evento. Secondo la tesi restrittiva, invece, il medesimo fatto dannoso ricorre solo in presenza di eventi collegati da equivalenti criteri di imputazione, per cui in caso di colpa la connessione si estende a tutti gli eventi prevedibili (se ben capisco): M. Orlandi, *La responsabilità solidale. Profili delle obbligazioni solidali risarcitorie*, Milano, 1993, 156-161. Seguono questo secondo orientamento: - S. Marullo di Condoianni, *Art. 2055*, in U. Carnevali (a cura di), *Dei fatti illeciti, Art. 2044-2059*, in E. Gabrielli (dir. da), *Comm. del cod. civ.*, Torino, 2011, 439-440 (limitando però l'art. 2055 al caso di concorso colposo ed escludendolo in quello di concorso tra illecito doloso e colposo, come sarà frequente nella materia qui esaminata: 447 ss.); - sostanzialmente anche A. D'Adda, *Le obbligazioni plurisoggettive*, in F. Anelli-V. Roppo-P. Schlesinger (dir. da), *Tratt. dir. civ. comm. Cicu Messineo*, Milano, 2019, 47 ss., §§ 12-14: per questo a. il medesimo fatto dannoso ex art. 2055 c.c. richiede la non separabilità degli effetti (di ciascuna condotta) e un reciproco coordinamento (prevedibilità) delle condotte. Il requisito della non separabilità mi pare presupposto da chi afferma che la solidarietà risarcitoria ex art. 2055 c.c. si applica a responsabilità che son già di per sé <<integrali>> (ciò che non ricorre quando le conseguenze sono separabili): detta norma non si limita quindi ad unificare una serie di responsabilità individuali che –in mancanza- risultino frazionate tra i diversi autori (S. Balbusso, *Il regresso nella solidarietà risarcitoria*, Milano, 2016, 143)

[29] Bocchini R., *La responsabilità civile degli intermediari*, cit., p. 201. Sulla *secondary liability* v. Riordan J., *The liability of internet intermediaries*, cit., 116 ss. (in generale),, 132 ss (in tema di copyright, e spt. 141 ss per gli ISP), 164 s per i marchi e concorenza sleale decettiva, p. 227 ss e 242 ss (per diffamzioni), 270 ss per violaziin di riservatezza.

persone>>: la sua formulazione è dunque così lata, da permettere il concorso eventuale sopraggiunto.

Naturalmente, precisa questa dottrina, l'eventuale responsabilità solidale del provider è limitata alle conseguenze risarcitorie, derivate dalle condotte tenute dopo la violazione a lui imputabile: e cioè -lo ripeto- dopo il momento, in cui è sorto il dovere di rimozione. Non può estendersi, invece, a quelle derivate dalla condotta anteriore, le quali graveranno solamente sull'utente. E' vero che anche in queste ultime c'è il fatto materiale del provider, dato che per definizione il suo servizio è proprio lo strumento utilizzato per la violazione: tuttavia, fino a che non sorge il dovere di rimozione, il provider non è soggetto ad alcun dovere e la responsabilità è allora monosoggettiva, id est in capo al solo utente. Il che presenta due interessanti profili: i) nei rapporti interni si applicherà conseguentemente l'art. 2055 c. 2-3, secondo cui <<colui che ha risarcito il danno ha regresso contro ciascuno degli altri, nella misura determinata dalla gravità della rispettiva colpa e dall'entità delle conseguenze che ne sono derivate. Nel dubbio, le singole colpe si presumono uguali>>: e sarebbe interessante ragionare sul punto; ii) toccherà al soggetto leso individuare la porzione di danno imputabile alle due fasi dell'illecito (monosoggettivo/plurisoggettivo), dato che la questa distinzione ha rilevanza esterna. Se la si ritenesse invece rilevante solo internamente –cioè in sede di regresso-, allora l'illecito sarebbe ab initio plurisoggettivo: ma questo contraddirebbe il punto di partenza, in base al quale al provider non si può addebitare nulla prima del momento in cui sorge il suo dovere di rimozione/disabilitazione.

L'operazione di imputazione delle due porzioni di danno potrebbe sembrare difficile, ma non è detto che sarebbe poi così: già oggi le liquidazioni tengono conto della durata dell'esposizione on line del materiale illecito. Si tratterà quindi solamente di aggiungere al calcolo il primo periodo cioè quello dell'illecito a struttura monosoggettiva, sempre che si agisca pure verso l'utente (eventualità più che rara, a quanto consta): altrimenti si terrà conto solo dell'esposizione a partire dalla presa di consapevolezza in capo al provider (in pratica: dal suo ricevimento di comunicazione/diffida da parte del soggetto leso).

3. Responsabilità contrattuale o aquiliana?

Negli scritti in materia si dà per scontato che, oltre a quella dell'utente, anche la condotta del provider (nella ricordata modalità omissiva) costituisca una violazione del neminem laedere e quindi censurabile ai sensi del 2043 cc, in combinato disposto con le norme che pongono i diritti violati. Il punto merita un approfondimento. Se la responsabilità aquiliana consegue ad una condotta violatrice di interessi protetti in assenza di una previa relazione tra le parti, mentre quella contrattuale sorge dall'inadempimento di un dovere che legava creditore e debitore, la conclusione –tralaticia-, per cui nel caso de quo ricorre responsabilità aquiliana, è da verificare. Ed anzi si può arrivare ad una conclusione parzialmente opposta.

Il ragionamento potrebbe svilupparsi così. La condotta del provider è una condotta omissiva, nel senso che gli si addebita di non aver rimosso o disabilitato (di seguito per brevità scriverò di "rimozione/disabilitazione" per indicare le due possibilità di intervento da parte del provider indicate dalla legge[30]). In generale, l'obbligo violato, fonte di responsabilità contrattuale, può avere fonte pattizia o legale (l'espressione responsabilità contrattuale è una sineddoche)[31], nel senso che l'inadempimento in entrambi i casi è governato dagli articoli 1218 e seguenti. Quindi la distinzione si basa sulla ravvisabilità o meno di un previo rapporto tra le parti, tale per cui la condotta censurata costituisca inadempimento ad un obbligo da esso sorto[32].

Nel caso specifico, come detto, si parte dal presupposto per cui, fino a quando il provider non sa della violazione, nulla gli può essere addebitato; da quando sa della violazione, invece, sorge a suo carico l'obbligo di rimozione[33]. Ne segue che, quando questo sorge, la sua violazione diventa appunto

[30] "Per rimuovere le informazioni o per disabilitarne l'accesso": così sia nel d. lgs. 70 che nella dir. versione italiana.

[31] Breccia U. *Le obbligazioni* in *Tratt. dir. priv.* Iudica Zatti, Giuffrè, 1991, 665; Bianca C.M., *Dir. civ. 5): la responsabilità*, Giuffrè, 2 ed., 2012, p.1; Giardina f., *Responsabilità contrattuale e responsabilità extracontrattuale. Significato attuale di una distinzione tradizionale*, Giuffrè., 1993, 140.

[32] Per questo si parla di responsabilità primaria per quella aquiliana e secondaria (o derivata) per quella contrattuale.

[33] Non conta ora appurare quando possa affermarsi la conoscenza del provider: lo si vedrà dopo.

violazione di tale obbligo: il quale mira ad evitare lesioni[34] della sfera di un soggetto ben determinato (il soggetto leso, normalmente autore della diffida). In altre parole, in assenza di un obbligo generale di sorveglianza, il dovere di rimuovere sorge solo quando gli venga segnalata una violazione specifica: violazione cioè di una situazione giuridica soggettiva protetta in capo ad un soggetto determinato[35]. Il dovere di rimuovere, dunque, non è più una cautela a favore della collettività, come sarebbe se gravasse sul provider un dovere generale di sorveglianza (in sostanza, sarebbe allora vicina alla responsabilità editoriale): è invece un dovere che mira a tutelare specificamente la posizione del soggetto leso, la lesione della cui sfera gli è stata notificata. Questo dovere crea dunque una relazione ben individuata tra provider e soggetto leso, relazione che mira alla tutela di quest'ultimo. Ne segue che l'omissione di rimozione costituisce violazione del dovere a carico del provider e a favore del soggetto leso: quest'ultimo diventa creditore della prestazione di rimozione/disabilitazione. Più che di dovere (soggettivamente) generico, allora, è esatto parlare di obbligo (soggettivamente) specifico [36].

In senso contrario potrebbe dirsi che le disposizioni normative (d. lgs. 70/2003 e dir. 2000/31) non pongono un obbligo ma un onere: come si dirà poco sotto, infatti, si limitano a dire che il provider non può essere tenuto responsabile se non sa o, qualora sappia, se procede subito a rimozione/disabilitazione. Il che pare costituire un onere per la fruizione del safe harbour. Non si dice infatti -in positivo- che il provider, quando sa, deve procedere a

[34] Rectius, ad evitare il protrarsi di quella già realizzatasi: la messa on line è già lesione, anche se nessuno la notasse.

[35] Così per il DMCA statunitense: Matteson J.D., *Unfair Misuse: How Section 512 of the DMCA Allows Abuse of the Copyright Fair Use Doctrine and How to Fix It*, in *Santa Clara high. tech. jour*., 2018, vol. 35/2, 9.

[36] Se si accetta di riservare il <<dovere>> ai casi, in cui beneficiari del contegno non sono soggetti determinati come creditori (Castronovo C., *Responsabilità civile*, cit., 534). "Obbligo", poi, rispetto ad "obbligazione", indicherebbe i vincoli che derivano dalla legge (Gambino F., *Il rapporto obbligatorio*, in *Tratt. dir. civ.* dir. da Sacco, 2015, 30-31): ma c'è il rischio di confusione concettuale, dato che per altri la distinzione i due termini sta invece nella patrimonialità della prestazione dedotta nella seconda (Ruperto S, *La dinamica giuridica. Un itinerario di diritto privato*, Giappichelli, 2019, 103: "dovere" sarebbe il termine più ampio in assoluto, essendo riferibile anche ai vincoli sociali e morali).

rimozione/disabilitazione; si dice invece che così deve fare, se vuole fruire dell'irresponsabilità. Potrebbe dunque dirsi che la legge resta muta sui doveri (generici –responsabilità aquiliana- o specifici –responsabilità contrattuale-) del provider, anche dopo esser stato notiziato dell'illecito: potrebbe dirsi cioè (fermo restando che, se non rimuove/disabilita, perde il safe harbour) che egli tuttavia non avrebbe un obbligo in senso tecnico di agire in tale senso.

Tuttavia il dovere di solidarietà, che innerva tutti i rapporti sociali, porta ad una conclusione diversa. Visto che dipende da lui e solo da lui la protrazione della condotta illecita (e la produzione di eventuali danni ulteriori al soggetto leso), il provider deve attivarsi per farla cessare. La diligenza professionale –che gemma da tale solidarietà- implica che nello svolgimento della propria attività il professionista si sforzi di non causare danno ai terzi con cui viene a contatto.

A ciò induce pure la considerazione complessiva delle disposizioni *de quibus*. Queste, pur mirando ad alleggerire e chiarire gli obblighi dei provider, hanno ritenuto di negare il safe harbour quando egli, pur sapendo di uno specifico fatto lesivo, non abbia rimosso o disabilitato. Se ne deduce che questa omissione è ritenuta grave dall'ordinamento: per cui è incongruo ravvisare solamente l'effetto della perdita del safe harbour e non anche l'illiceità (e la conseguente soggezione ai pertinenti rimedi). Che le disposizioni europee si siano limitate a porre una disciplina in negativo (safe harbour) deriva probabilmente dalle rilevanti difficoltà di conciliare ordinamenti diversi su un tema complesso come la responsabilità civile, seppur solo per l'attività degli ISP: optandosi quindi per un'armonizzazione più limitata, consistente nella perimetrazione appunto di un'esimente e cioè di un'area sicura per gli operatori del settore[37].

[37] Simile osservazione in Buiten M.-de Streel A.-Peitz M., *Rethinking Liability Rules for Online Hosting Platforms*, CRC TR 224 Discussion Paper Series CRC TR 224 n° 074, project B 05, University of Bonn and University of Mannheim, Germany, 2019, p.14. E' stato segnalato un conflitto disciplinare tra le norme de quibus (safe harbour ex dir. 2000/31), da un parte, e le direttive Enforcement 2004/48 e Infosoc 2001/29, dall'altro. Deriverebbe dal fatto che il dovere per gli Stati di istituire inibitorie, previsto nelle seconde (artt. 9 e 11, dir. 2004/48; art. 8.3, dir. 2001/29), contrasterebbe con le prime, dato che il safe harbour potrebbe intendersi come comprendente pure l'injunction (Leistner M., *Structural aspects of secondary (provider)liability in Europe*, *Journ. of int. prop. law pract*., 2014,

In breve, che un dovere di agire nel senso della rimozione/disabilitazione vi sia, non dovrebbe essere dubbio, quantomeno come dovere di cautela generica ex art. 2043. La condotta del provider infatti per definizione corre –sotto il profilo materiale- con quella dell'utente nel produrre il fatto dannoso (art. 2055): per cui l'omessa rimozione/disabilitazione, dopo l'avviso, costituisce negligenza. Il problema è piuttosto come costruire questo dovere e cioè se erga omnes oppure solo verso il soggetto leso. Se fosse giusta la seconda ipotesi, dovremmo optare per la responsabilità contrattuale: sarebbe incongruo rimanere nell'ambito aquiliano, quando il comportamento da tenere è già orientato verso la tutela di una ben precisa sfera individuale[38].

vol. 9/1, 76-77). Il conflitto pare in realtà non esistere, dato che: i) il safe harbour prevede la possibilità di inibitorie (c. 3 degli artt. 12, 13 e 14 dir. 2000/31), il cui concetto ad una prima lettura pare sostanzialmente uguale a quello delle due successive dirr.; ii) la dir. 2000/31 è fatta salva sia dalla dir. 2001/29 (anche se solo nel cons. 16) che dalla dir. 2004/48 (qui pure nell'articolato: art. 2.3): aspetto importante soprattutto per il divieto di *general monitoring*, che resta intatto. Potrà esserci semmai una differenza fattuale nei recepimenti nazionali, dato che l'inibitoria in alcuni ordinamenti può essere anche amministrativa (come prevede la dir.) e in altri solo giudiziale (in UK, come ricorda M. Husovec, *Injunctions aganist intermediaries in the European Union. Accountable but not liable?*, Cambridge University Press 2017, 116-117). Ma questo non implica alcun contrasto normativo: anzi la cennata possibilità è voluta, avendo l'UE optato per la dir anziché per il regolamento.

[38] Come detto sopra e noto, la responsabilità aquiliana riguarda il pregiudizio arrecato tra soggetti non legati da alcun rapporto e cioè riguarda impatti occasionali (v. ora Montanari A., *Il danno antitrust*, Cedam, 2019, 279-284, sulla scia di Castronovo). Ci sono però visioni diverse. Ad es. per Navarretta E., *L'ingiustizia del danno e i problemi di confine tra responsabilità contrattuale e extracontrattuale*, in *Dir. civ.* dir. da Lipari e Rescigno, coor. da Zoppini, Giuffrè, vol. IV.III, *La responsabilità e il danno*, Giuffrè, 2009, 235-236, per cui la relazionalità è compatibile con la responsabilità aquiliana, come proverebbe soprattutto l'art. 11 d. lgs. 196/2003 (cod. privacy, testo orig.), disposizione secondo cui i dati vanno trattati con "correttezza". La sua tesi non persuade, tuttavia, dato che i) il richiamo alla correttezza nulla dice sulla qualificazione, limitandosi a riassumere i tipi di contegno che il titolare del trattamento deve tenere, a prescindere dal tipo di relazione con i soggetti, i cui dati tratta (nulla significa il fatto che di correttezza il codice civile parli soprattutto nel libro delle obbligazioni, essendo menzionata anche in fattispecie aquiliane, come nella concorrenza sleale ex art. 2599 o nei doveri degli amministratori circa le operazioni con parti correlate ex art. 2391 bis c. 1); ii) la responsabilità da illecito trattamento dei dati, poi, mi pare contrattuale, in quanto -trattandosi di soggetti determinati- gli obblighi verso di loro poggiano su una relazione giuridicamente rilevante da subito e non solo in caso di violazione. E' vero che un minimo di relazionalità ricorre spesso anche nella responsabilità aquiliana: come ad es. nel

In altre parole, ritenere che il dovere rimanga tra quelli generici, propri della responsabilità aquiliana, non soddisfa. Il provider, quando è avvisato del file illecito presente sui suoi server, non può più ritenersi gravato verso il soggetto leso dallo stesso dovere di neminem laedere, che ha verso il resto della collettività (o meglio verso il resto delle persone, i cui dati sono trattati nei file da lui ospitati). Il suo rapporto con la sfera del soggetto leso è assai diverso da quello che ha con questi ultimi, dato che il primo infatti si staglia nettamente nella folla indistinta dei secondi. Il dovere di rimozione/disabilitazione allora si precisa e concretizza a favore di uno soggetto determinato, di cui il provider viene a conoscere[39] -combinando l'esame della diffida con quello del file illecito - nome, cognome, situazione giuridica lesa, modalità lesiva e magari altri dati ancora (posizione giuridica, posizione sociale...). Il contatto tra il primo e il secondo è dunque ben più consistente di quello tipicamente aquiliano: il quale può forse consistere anche in qualcosa di più della "responsabilità del passante", ma non arrivare al punto da comprendere quello in cui l'autore della condotta dannosa può fare quella valutazione personalizzata (non generica, come quella ipotizzabile in astratto erga omnes) della sfera altrui,

caso di due automobilisti, i quali, dapprima "guardatisi" con fastidio o addirittura sfida, se poi collidono, generano reciproca responsabilità aquiliana, non contrattuale. Si tratta però di relazione debole, ad es. perché non sono reciprocamente individuati restando anonimi (ma nulla cambierebbe se si conoscessero). Né la menzione della correttezza nell'art. 2598 n. 3 presuppone una relazione significativa tra concorrenti, tale da smentire che la responsabilità aquiliana cocnerna i contatti occasionali (così invece Navarretta E., *L'ingiustizia del danno*, op. loc. cit.): non esiste infatti alcun dovere specifico tra due concorrenti determinati prima del compimento dell'atto sleale (è irrilevante che nei fatti le slealtà vengano attuate tra soggetti che si conoscono, magari anche bene), al pari delle norme del codice della strada, che impongono <la massima prudenza> (ad es. art. 145 c. 1) oppure di <comportarsi in modo da non costituire pericolo o intralcio per la circolazione ed in modo che sia in ogni caso salvaguardata la sicurezza stradale> (art. 140 c. 1), le quali non fanno sorgere obblighi reciproci tra soggetti (pre-)determinati. Del resto anche il reato doloso può prevedere una qualche relazionalità, dato che viene preparato per tempo, magari all'interno di rapporti sociali precisi: ma civilisticamente resta torto, non inadempimento di obbligo (interessante il caso in cui si inserisca in relazione ad es. familiare, in cui dei doveri tra i soggetti esistono). Il confine però non è netto, dipendendo anche dalla temperia culturale del momento (Bussani M., *L'illecito civile*, cit., 67).

[39] Di solito dal medesimo soggetto leso tramite intimazione di pronta rimozione/disabilitazione.

coinvolta dal suo agire commissivo od omissivo, che sta alla base della diversa disciplina contrattuale rispetto a quella aquiliana. Si pensi al mancato richiamo nell'art. 2056 dell'art. 1225, che limita il danno a quello prevedibile al momento del sorgere dell'obbligazione: è ingiusto infatti gravare il debitore di ciò che, secondo un criterio di normalità, non poteva prevedere[40], dovendosi rispettare solo il programma contrattuale

[40] Pacifico in dottrina: Franzoni M., *Tratt. della responsabilità civile. Il danno risarcibile*, Giuffrè, 2004, 10-11; C.M. Bianca, *Dir. civ. 5) la responsabilità*, 2 ed.,Giuffrè, 2012, 171 e 786. La diversità disciplinare però si riduce assai, se si tiene conto che il danno risarcibile di solito è ravisato entro i limiti della regolarità causale (lo nota Bianca, cit., 786, nota 2). Anzi, è la stessa generale distinzione tra responsabilità contrattuale ed aquiliana a dover essere ridotta, trattandosi sempre di scostamento dalla condotta dovuta (in base alle pattuizioni o alla diligenza appropriata alle circostanze). Per cui ad es. la differenza di onere probatorio, stante la concezione normativa della colpa –in realtà elemento assente nella responsabilità contrattuale, come già spiegarono Osti e Mengoni e successivamente Castronovo ed altri- si riduce alla (possibile) differenza di parametro (agente-modello) per valutare la condotta tenuta: parametro che è modulabile dalle pattuizioni solamente nella responsabilità contrattuale e che invece coincide nelle due responsabilità, se in quella contrattuale mancano speciali patti, dato che ci si riferirà sempre al medio *homo eiusdem professionis et condicionis*. Un'impostazione simile, sulla base della concezione c.d. oggettiva della responsabilità contrattuale, leggo in Visentini G., voce *Responsabilità contrattuale ed extracontrattuale*, Enc. giur. Treccani, XXVI, 1990, p. 3, § 3 (distinguendo però sul parametro di riferimento in modo non del tutto condivisibile). Non persuade la replica a Visintini mossa da Anzani G., *Il riparto dell'onere probatorio nelle due specie di responsabilità civile*, *Riv. trim. dir. proc. civ*., 2017, p. 233, nota 16, secondo cui rimarrebbe la differenza per cui nella responsabilità contrattuale il creditore non è onerato di provare che l'inadempimento è stato causato da causa imputabile al debitore: alla luce della cit. concezione normativa della colpa (inevitabile, non potendosi scrutare l'"interno foro" altrui; sull'oggettività del paramentro della colpa aquiliana v. Castronovo C., *Responsabilità civile*, Giuffrè, 2018, 19 e 408), infatti, anche nella responsabilità aquiliana al danneggiato basta provare lo scostamento dalla condotta che avrebbe dovuto essere tenuta da un agente-modello, la quale comprende sia la condotta "ordinaria" o "normale", sia quella "anormale" o "extraordinaria", che sarà più o meno diversa dalla prima in base alle circostanze (allo stesso modo in cui, nella responsabilità contrattuale, va abbandonata la distinzione tra prestazione dovuta -in senso stretto- e cautele da adottare per conservarne la possibilità di adempimento, anche queste facenti parte della prima *pleno titulo*). Svaluta la distinzione tra le due tradizionali forme di responsabilità anche Maggiolo M., *Il risarcimento della pura perdita patriminiale*, Giuffrè, 2003, p. 100 ss., §§ 26-31 (svalutando addirittura pure la differenza più significativa, costituita dal diverso termine prescrizionale, basandosi sulla permanenza dell'illecito: p. 125 ss). Responsabilità da inadempimento e da fatto illecito "*sono tra loro molto più simili di quanto non lo sia ciascuna di esse rispetto a singole fattispecie di responsabilità di settore che pure all'una o all'altra si ispirqano. Gli attuali contorni della distinzione … sono assai più*

o lo scenario che le parti si erano prospettate esplicitamente o implicitamente quando fecero sorgere l'obbligo[41]. Criterio che non vale per l'illecito aquiliano, in cui non ricorre alcun impegno determinato e dunque alcuna normalità prevedibile[42]. Se così è, il provider, quando viene notiziato e intimato di procedere a rimozione/disabilitazione perché un file da lui ospitato viola un certo diritto in capo ad un soggetto determinato, può fare il calcolo di costi e benefici delle alternative del suo agire: il suo dovere di rimuovere/disabilitare è a favore di un soggetto preciso, non della indistinta massa dei *cives*. Ricorre insomma quel "rischio specifico" che permette di ricondurre il contatto de quo alla responsabilità contrattuale, invece che a quella aquiliana[43]. Quest'ultima è caratterizzata dall'assenza di obblighi verso persone determinate, sicchè chi non è da essi vincolato è libero, fino a quando leda il diritto altrui (tranne l'inibitoria): lesione che determina il sorgere dell'obbligazione

sfumati rispetti ai rigidi termini della contrapposizione tradizionale"; ed anzi il "*rapporto obbligatorio originario appare dunque fattore di <<specificazione>> della responsabilità: questo fa sì che si crei un rapporto di genere a specie tra responsabilità aquiliana e responsabilità debitoria, responsabilità generale di diritto comune la prima, specificazione della regola generale in presenza di un rapporto obbligatorio la seconda*" (così Giardina F., *Responsabilità contrattuale e responsabilità extracontrattuale. Significato attuale di una distinzione tradizionale*, Giuffrè, 1993, 232 e risp. 234)

[41] Così sostanzialmente anche A. D'Adda, *Riflessioni sul risarcimento del danno (im)prevedibile*, in *Riv. dir. civ*., 2019/6, 1298. Questo a. analizza poi il dubbio di sovrapponibilità (escludendola) tra prevedibilità dei danni ex art. 1225 e risarcibilità solo entro la <<conseguenza immediata e diretta>> ex art. 1223.

[42] L'inadempimento doloso, che pure osta alla limitazione al danno prevevibile, costituisce un atteggiamento che fuoriesce dal programma contrattuale, sicchè ha piuttosto natura di illecito aquiliano: due profili che invece certa dottrina (A. D'Adda, *Riflessioni sul risarcimento del danno (im)prevedibile*,cit., cit., 1313) tiene distinti, anche se il secondo mi pare discendere dal primo o meglio sia la conseguente qualificazione del primo. La differenza operativa tra il risarcimento del danno contrattuale ed aquiliano, in relazione al mancato richiamo dell'art. 1225, è però tutta da verificare: infatti si giungerà spesso anche nella seconda ipotesi a non caricare l'autore dell'illecito delle <<*conseguenze dannose che appaiono lontane dal suo agire ogni qual volta egli, al momento di entrare in azione, non abbia avuto la possibilità di prevederne l'occorrere*>> (così Bussani M., *L'illecito civile*, cit., 71-72); anche se si largheggia nel ravvisare la prevedibilità quando ricorra il dolo (Bussani M., *L'illecito civile*, ivi, 644 e 666/7).

[43] Così Iuliani A., *Obblighi strumentali azione di adempimento,* Giuffrè Francis Lefebvre, 2018, nota 45, a proposito della responsabilità contrattuale per violazione dell'affidamento creato dallo status, nota tesi di Castronovo.

(risarcitoria)[44]. Ebbene, stona riconoscere questa libertà al provider, dopo che è stato notiziato della lesione arrecata da file presenti sul suo server.

C'è una differenza rispetto ai casi consueti di obbligazione senza prestazione, sorta da contatto sociale. In questi infatti il contatto è allacciato dalla parte poi lesa, la quale legittimamente "si affida" all'altro; nel caso nostro, invece, l'affidamento non sorge da previo contatto, allacciato dal soggetto leso, ma è creato dalla legge e cioè dal dovere di solidarietà costituzionale gravante su chi, pur non essendo l'originario uploader, può tuttavia bloccare senza fatica la permanenza dell'illiceità. Inoltre nel caso de quo la condotta dovuta, che soddisfa l'affidamento, consiste non nell'informare ma nel rimuovere. L'ordinamento non resta impassibile di fronte alla situazione, in cui il rischio di danno sorge dall'attività di un preciso soggetto (internet provider), il quale quindi può governarlo ed anzi azzerarlo: l'art. 2 Cost. gli impone allora quel minimo comportamento collaborativo, che, se a volte può consistere in un mero dovere di informazione[45], nel nostro caso consiste nella rimozione/disabilitazione.

Potrebbe dirsi in senso contrario che, per costruire un dovere di attivarsi, servisse una norma specifica e/o espressa: la quale, in altre parole, sarebbe necessaria per ritenere illeciti i contegni omissivi. Ciò soprattutto a tutela della libertà personale, che potrebbe essere pericolosamente ridotta dalla ravvisabilità di doveri di azione impliciti, invece che espliciti: questa è la ragione per cui -secondo l'art. 23 Cost.- "nessuna prestazione personale o patrimoniale può essere imposta se non in base alla legge". Quella addossata al provider sarebbe appunto una

[44] Così Castronovo C., *Responsabilità civile*, Giuffrè, 2018, 533.

[45] Simile osservazione in Gigliotti F., *Illeciti da inforormazione e responsabilità omissiva*, Riv. dir. civ., 2002, I, 919-928, passim: da un lato, chi, con la sua ttività (anche lecita) crea un rischio per un terzo, ha l'obbligo di avvisarlo appena ne viene a conoscenza; dall'altro, se il terzo è soggetto determinato, la violazione genera responsabilità non aquiliana ma contrattuale (p. 928 e rispett. 917/8). Prospettiva accolta in Iuliani A., *Obblighi strumentali*, cit., 294, in termini di responsabilità aquiliana quando si tratta di rischio creato o origintosi nela sfera di controllo del responsabile (non menziona la questione dell'altenativa in termini contrattuali); con diversa soluzione quando si tratti di "rischio altrove creato" (non nella propria sfera, parrebbe), eventualità in cui l'affidamento fa sorgere obblighi cooperativi solo in presenza di affidametno sorto da preesistente relazione (ivi, p. 294-297).

prestazione personale.

Il punto è delicato, essendo la libertà bene preziosissimo: pare però che il garantismo liberal-ottocentesco possa essere in certi casi superato. L'art. 1173 c.c, ad es., non si riferisce più alla "legge" ma al più ampio concetto di "ordinamento giuridico", nel quale rientrano oggi anche i principi costituzionali, tra cui quello di solidarietà e di rispetto di sicurezza, libertà e dignità umana[46]. Da questi può farsi sorgere un dovere di azione in casi come quello de quo, poiché attendere la lesione dannosa, per potersi difendere, pare difforme dai principi medesimi. Il danno da attesa per il soggetto leso può essere molto rilevante, mentre è minimo per l'internet provider quello del doversi attivare (anche perché può cautelarsi redigendo opportuni moduli, quando allaccia rapporti contrattuali con i suoi utenti): per questo il bilanciamento è a favore del soggetto leso. Non si tratta qui tanto di bilanciamento tra due sfere toccantesi, per vedere se il danno cagionato da una verso l'altra sia ingiusto; si tratta di bilanciarle per vedere se ex ante –cioè prima che un danno sorga o si estenda- possa ravvisarsi un'obbligo di attivarsi per evitare il danno (o il suo incremento), altrimenti assai probabile e spesso (diffamazione) di fatto non più eliminabile né ristorabile.

Ci sono del resto diverse norme che interessano il discorso

[46] In tal senso molta dottrina, la quale si divide su alcuni aspetti: ad es. sulla diretta invocabilità dei principi costituzionali oppure sulla necessità di rimanere ancorati alle regole interpetative consuete del necessario ricorso all'analogia o ai principi generali ex art. 12 prel (la differenza in concreto si riduce assai, se si tien conto che questi ultimi sono enucleabili anche dalle norme in Costituzione). Nel primo senso v. Di Majo A., *sub art. 1173*, in *Comm. Scialoaa Branca* a cura di Galgano, artt. 1173-1176, Zanichelli 1988, 171 ss, spt. 175 e 177/8 e Rescigno P.., voce *Obbligazioni*, *Enc. dir.*, Giuffrpè, XXIX, 1979, 151/2. Li seguono: F. Gazzoni, *Manuale di diritto privato*, XII ed., ESI, 2006, 575/6; Breccia U., *Le obbligazioni*,in *Tratt. dir. priv. Iudica Zatti*, Giuffrè, 1991, 110 e 114; Bianca CM, *Diritto civile. 4) l'obbligazione*, Giuffrè, 1990, 6, nota 12; Albanese A., *Il rapporto obbligatorio: profili strutturali e funzionali*, Libellula ediz., 2014, pp. 33-36. Nel secondo senso, Gambino F., *Il rapporto obbligatorio*, cit., cap. 2°, passim (ad es. 47, 67, 79 ss, 89/90.111-114 e soprattutto p. 85-86). Ammette l'atipicità delle obbligazioni da fatto lecito Cannata C. A., *Le obbligazopni in generale, Tratt. dir. priv.*, vol. *9 Obbligaioni e contratti*, t. 1, 2 ed., 1999, rist. 2005, 25/6, che però le limita all'ambito dei quasi contratti (p. 27/8). Sul problema dell'efficacia orizzontale delle norme di rango costituzionale (*Drittwirkung*) v. ora i saggi di Zoppini, Navarretta e Plaia in Mezzanotte F. (a cura di), *Le «libertà fondamentali» dell'Unione europea e il diritto privato*, Roma Tre-Press, 2016 nonché quelli di Libertini e Resta in Caggia F.-Resta G. (a cura di), *I diritti fondamentali in Europa e il diritto privato*, 2019.

che si va conducendo, che richiederebbero esame analitico, qui non possibile. Mi limito qui ad elencarne alcune:

1) dovere di prestare assistenza o avvisare l'autorità, penalmente sanzionato dal reato di omissione di soccorso, art. 593 c. 1-2 c. pen.;

2) potere di Consob di ordinare l'oscuramento telematico di chi <<offre o svolge servizi o attività di investimento senza esservi abilitato>> (art. 36 c. 2 terdecies d.l. d. l. 34 del 30.04.2019 (conv. da legge n. 58 del 28 giugno 2019).

3) potere del Ministero Finanza-Monopoli si Stato di ordinare l'oscuramento (in modalità lasciate a decreti successivi) in caso di attività di gioco on line non autorizzate (art. 1 c. 50-50 quater, L. 27-.12-2006 n. 296, finanziaria 2007)

4) potere dell'autorità giudiziaria procedente di ordinare l'oscuramento di siti internet in tema di terrorismo internazionale (art. 2 c. 3-4 d.l. 18.02.2015 n. 7 conv. da L. 17.04.2015 n. 43).

5) diritto di chiedere l'oscuramento in caso di cyberbullismo con seguente possibilità –in casi di omissione- di adire il Garante privacy (art. 2 l. 71 del 29.05.2017)[47].

6) qualificazione imperativa di illiceità nella condotta del provider del mero conservare file illeciti, caricati dagli utenti, sui propri server contenute nell'art.17 della dir. copyright 2019/790: è stabilito di imperio che ciò costituisce comunicazione al pubblico (a meno che riesca a liberarsi provando l'esistenza dei requisiti del § 4) (su ciò v. l'ultimo paragrafo)..

I casi da 2-3-4 pongono doveri pubblicistici, a tutela preventiva della collettività indistinta, per cui non ci interessano

[47] Qui ricorre una seria difficoltà nel determinare l'ambito soggettivo di applicazione della legge 71/2017. Secondo l'art. 1 c. 3, <<*per «gestore del sito internet» si intende il prestatore di servizi della societa' dell'informazione, diverso da quelli di cui agli articoli 14, 15 e 16 del decreto legislativo 9 aprile 2003, n. 70, che, sulla rete internet, cura la gestione dei contenuti di un sito in cui si possono riscontrare le condotte di cui al comma 2*>> (si deve vedere però pure l'art. 2 sulla legittimazione passiva dell'istanza). Pare tuttavia incongrua un'interpretazione letterale, secondo cui tutti coloro, che "gestiscono contenuti" (quindi anche "altrui"), soano esentati dalla disciplina de quo solo che ricadano nel *safe harbour* ex d. lgs. 70/2003. V. l'interpretaziopne correttiva proposta da Bocchini R.-Montanari M., *Le nuove disposizioni a tutela de oiminori per la prevenzione ed il contrasto del fenomeno del cyberbullismo (l. 29 maggio 2017 n. 71),* in *Nuove leggi civili commentate*, 2018/2, 340 ss., § 5 (spt. 364).

direttamente. I casi 1 e 5 invece pongono doveri a protezione di soggetti determinati. Se il caso sub 1 è dubbio fuoriesca dalla responsabilità aquiliana, il caso sub 5 invece dovrebbe rientrare in quella contrattuale: il dovere di provvedere, la cui omissione permette i poteri sostitutivi del Garante, riguardando un dovere giuridico verso un soggetto determinato e non verso la collettività indistinta, è del tutto analogo al nostro caso[48]: gli si può infatti applicare il ragionamento di cui sopra, che fa propendere per una responsabilità contrattuale. Circa il caso sub 5, però, può sorgere il dubbio che non vi sia un obbligo in senso tecnico in capo al provider, data l'equivoca formulazione e l'assenza apparente di sanzioni per il caso di inottemperanza: la disciplina potrebbe far pensare ad una mera condizione di procedibilità, per chiedere poi al Garante l'esercizio dei poteri di intervento. Se la ragione è quella di economia procedurale, e cioè di tentare le vie brevi prima di mettere in moto il procedimento amministrativo presso il Garante, pare ugualmente incongruo rimettere alla potestatività mera del provider la scelta del se accogliere o meno l'istanza. Parrebbe dunque sensato ravvisare un obbligo[49].

Pecca dunque di precisione un provvedimento di merito del 2015, pur interessante per i riferimenti tecnici alle possibilità di filtraggio e per alcuni condivisibili affermazioni ad esso legate: *<<Non pare inopportuno, poi, rammentare che la relazione che lega il titolare del diritto di proprietà intellettuale violato e il fornitore di servizi della società dell'informazione, non vincolati fra loro da alcun rapporto contrattuale, va collocata sul piano extracontrattuale e pare opportunamente catalogabile in termini di relazione da "contatto sociale", chiamando così i soggetti interessati a comportarsi secondo correttezza e buona fede, in prospettiva solidaristica, con la consapevolezza del*

[48] Anzi è identico, tranne che per il tipo di diritto violato.

[49] Tralascio l'esame della poco curata disciplina dell'ambito soggettivo passivo di applicazione dell'istanza. Da un lato, questa, secondo l'art. 2 L. 71/2017, può venir inoltrata *<<al titolare del trattamento o al gestore del sito internet o del social media>>*; dall'altro, *<<per «gestore del sito internet» si intende il prestatore di servizi della societa' dell'informazione, diverso da quelli di cui agli articoli 14, 15 e 16 del decreto legislativo 9 aprile 2003, n. 70, che, sulla rete internet, cura la gestione dei contenuti di un sito in cui si possono riscontrare le condotte di cui al comma 2>>* (art. 1 c. 3). In prima approssimazione, pare solamente volere fare salvo il safe harbour posto dalle citate disposizioni del d. lgs. 70/2003.

carattere funzionale dei diritti riconosciuti dall'ordinamento (cfr. art.2 Cost.) che limita intrinsecamente il loro agire alla luce del dovere generale di protezione dei diritti altrui. (..) Nella gestione del contatto sociale le parti sono chiamate a interagire, in prospettiva solidaristica, e quindi proteggendo gli interessi altrui, ove ciò sia possibile senza consistente pregiudizio dei propri, rifuggendo da declinazioni emulative dei propri diritti e garanzie che l'ordinamento riconosce loro in un'ottica funzionale e sociale>>[50]. Parlare di responsabilità da contatto sociale come applicazione di responsabilità aquiliana è sorprendente, anche se ha qualche antecedente giurisprudenziale[51]. La teoria del contatto sociale, infatti, consiste proprio nel portare una fattispecie di per sé aquiliana – per assenza di titolo contrattuale- in ambito contrattuale: ciò a causa del legame particolare e stretto, fonte di affidamento, tra il soggetto leso e l'autore della lesione[52], ovvero per la particolare prossimità del soggetto leso con l'ambito esecutivo di una prestazione, che l'autore della lesione stava rendendo ad

[50] Trib. Torino 03.06.2015, ord. cautelare, *Delta TV c. Dailymotion*, RG 2015/11343, p. 19. Nel caso specifico, poi, l'affermazione del giudice non concerne il dovere di rimozione/disabilitazione dopo la prima comunicazione del soggetto leso, ma quello di dar corso ad inibitoria giudiziale per condotte future: situazione in cui la delimitazione della diligenza solo verso un determibnato soggetto è allora giudizialmente sancita. Accenna a questa possibilità interepretativa pure Palazzo L., *La responsabilità per le violazioni su internet del diritto d'autore da parte degli utenti dei social network: la posizione dell'Internet Service Provider e del gestore del social*, 10.09.2020, in Law and Media Working Paper Series, n. 3/2020, in *medialaws.eu*, p. 10.

[51] Cass. III, 25.01.2011 n. 1737, ritenne responsabili in via aquiliana i proprietari di una macchina agricola per le lesioni e successivo decesso riportate da un terzo, che a titolo di cortesia era intervenuto per ripararla: la fonte della responsabilità fu ravvisata nella violazione del dovere di avvisare della pericolosità della macchina, dovere a sua volta fondato sulla solidarietà sociale. Ne dà notizia A. Zaccaria, *Der aufhaltsame Aufstieg des sozialen Kontakts (la resistibile ascesa del contatto sociale)*, in *Riv. dir. civ*., 2013, I, 105: l'a. rileva la contraddizione dell'usare una figura, nata per estendere la responsabilità contrattuale, per fondare invece un'affermazione di responsabilità aquiliana (p. 107).

[52] P. Gallo, voce *Contatto sociale e responsabilità medica*, Dig. disc. priv.-sez. civ., Agg. XII, 2019, 67 ss, § 1 e 3; Manna L., *Le obbligazioni senza prestazione*, in *La struttura e l'adempimento*, t. 3 a cura di Galogalo, in *Tratt. delle obbligazioni* dir. da Garofalo e Talamanca, Cedam, 2010, p. 6 ss.

un creditore terzo[53], prossimità che deve essere intenzionale[54]. Ebbene, un tale atteggiamento psichico è assente nel rapporto de quo: non esiste alcun volontario affidamento, né alcuna voluta prossimità intenzionale del soggetto leso verso la piattaforma. A parte ciò, secondo quanto appena osservato, il provider viola un obbligo già sorto verso un soggetto determinato, il quale diviene creditore della prestazione di rimozione/disabilitazione: non potendosi, dunque, parlare più di responsabilità aquiliana bensì di obbligazione ex lege.

E' dubbio che sia esatto ricorrere alla categoria della responsabilità (contrattuale) da contatto sociale anche perché questa di solito concerne casi, in cui il terzo è esposto a pericoli di danno uguali a quello di uno dei contraenti: qui invece l'utente utilizza i servizi del provider proprio ed unicamente per violare la sfera del soggetto leso. Quindi non ricorre l'esigenza di estendere la (più soddisfacente) tutela ex contractu, spettante al contraente, ad un soggetto terzo, che -per le circostanze del caso- si trova esposto al medesimo tipo di rischio di danno cui è

[53] Lambo L., *Obblighi di protezione*, Cedam, 2007, cap. V, spt. 290-294 e 304-309, per il quale il fondamento riposa sulla clausola di buona fede/correttezza ex art. 1175 cc in particolare, sulla falsariga della figura tedesca del contratto con effetti di protezione verso il terzo, fonte di obblighi autonomi da quello primario di prestazione (Id., *La responsabilità del medico dipendente e il gioco dell'oca (obblighi di poroteizone c. alterum non laedere)*, Il foro it., 2017, V, 242 ss., § 5; Nicolussi A., voce *Obblighi di protezione*, Enc. dir., Annali, VIII, Giuffrè, 2015, § 2: "*Inoltre, per quanto concerne i terzi, la solidarietà dà fondamento a una interpretazione estensiva dell'obbligo legale di protezione a favore di quei terzi che si trovino a partecipare del medesimo pericolo cui risulta esposta la parte in ragione del rapporto obbligatorio*" (in Dejure). La base giuridica dell'estensione del dovere protettivo verso soggetto diverso dal creditore, a dir il vero, rimane non sicurissima, essendo spesso individuata nell'affidamento che la professionalità di un soggetto genera nei terzi (Castronovo C., *Responsabilità civile*, cit., 559-572, circa la responsabilità del medico): è però da alcuni contestato che l'affidamento costituisca un principio generale in tale senso, operante anche oltre i casi espressi (Zaccaria A., *"Contatto sociale" e affidamento, attori protagonisti di una moderna commedia degli equivoci*, www.juscivile, 2017/3, § 5; Pittella D., *Dall'obbligazione senza prestazione alla responsabilità extracontrattuale del medico: rigetto locale o totale del contatto sociale "qualificato"?*, in *Contr. impr.*, 2020/1, 442), tutt'al più tramite cauta analogia rispetto al caso espresso della responsabilità precontrattuale ex art. 1337, a sua volta basata sulla violazione di un affidamento soggettivo, non oggettivo (Garofalo A.M., *Il problema del contatto sociale*, in *Teoria e storia del dir. priv.*, XI-2018, 336 ss spt. p. 43 e poi 110)..

[54] Piraino F., *La responsabilità precontrattuale e la struttura del rapporto prenegoziale*, in *Persona e mercato*, 2017/2, § 4, 125 ss.

esposto il contraente stesso. Pur tuttavia, come sopra, detto può ravvisarsi un obbligo in senso tecnico di rimozione/disabilitazione a carico del provider.

In quanto responsabilità contrattuale, si applicheranno le regole di cui all' articolo 1218 e seguenti, che in parte differiscono da quelle aquiliana. Le principali differenze, scolasticamente ripetute, riguardano: i) limitazione della responsabilità contrattuale ai danni prevedibili, tranne che ricorra dolo, art. 1225, non richiamato dagli artt. 2043 ss; ii) il termine prescrizionale, decennale per la responsabilità civile e quinquennale per la responsabilità aquiliana, art. 2947 cc; iii) la messa in mora, non necessaria quando si tratta di fatto illecito, art. 1219 c. 2 cc. La differenza non riguarda invece il giudizio di colpa/negligenza, la quale è sempre costituito dalla violazione della normale diligenza[55].

Circa l'art. 1225 va però segnalato che la regola del risarcimento limitato ai danni prevedibili non opera, se si segue la tesi per cui il provider, qualora non provveda a rimozione/disabilitazione una volta notiziato, è da ritenersi in dolo[56]. La tesi, ad una prima riflessione, non pare persuasiva, se si accetta che il concetto di dolo civilistico si modella su quello penalistico. Nell'art. 43 c.1. c.p., da un lato, <<*la qualificazione dolosa del reato rimanda espressamente all'intenzione e i poli costitutivi della responsabilità dolosa sono dati dalla previsione e dalla volizione dell'evento. Atteso che la previsione di quest'ultimo è compatibile anche con la responsabilità colposa (nella forma cosciente), la volizione dell'evento rappresenta la vera cifra identificativa del dolo*>>[57]; dall'altro, il giudizio non cambia in relazione ai reati omissivi, propri o impropri[58]. L'evento, nel caso di domanda risarcitoria, è il danno-conseguenza (ma nulla cambierebbe riferendoci al danno-evento): per cui è ben difficile sostenere che il provider abbia

[55] Bianca C.M., *Dir. civ. 5): la responsabilità*, cit., p. 560.

[56] Bocchini F., *La responsabilità civile plurisoggettiva, successiva ed eventuale dell'ISP*, nota a Cass. 19.03.2019, n. 7708, in Giur. it., 2019, 12, 2606 ss, a 2611 e 2613 nt. 26).

[57] Così M. Caputo, *Art. 43*, in *Codice penale* a cura di T. Padovani, t. 1, Giuffrè, 7 ed., 2019, 310, § 2. Il nostro caso costituisce un illecito omissivo improprio, essendo sanzionata l'omissione che lede (e danneggia) una sfera giuridica altrui.

[58] M. Caputo, *Art. 43*, cit., 313, § 6; G. Fiandaca, voce *Omissione (diritto penale)*, Digesto, 1994, in *Pluris*, sub § 5.B.a.

voluto arrecare danno al soggetto leso[59]. Ciò vale, a meno di ravvisare la figura del dolo eventuale, che ricorre quando, pur non volendo l'evento, tuttavia si continua ad agire accettandone il rischio: in tale ipotesi effettivamente si potrebbe sostenere che proprio questa è la fattispecie che ricorre quando il provider, pur notiziato, non rimuova e/o disabiliti. Ad es. potrebbe dirsi che l'inadeguata organizzazione del provider, con una scadente catena informativa (tra addetti al ricevimento comunicazioni esterne e decisori), tale da portare all'omissione, costituisse inefficienza tollerata proprio per non subire incrementi di costi: in tale caso sarebbe difficile disconoscere il dolo eventuale. Come del resto ed in generale può dirsi per tutti i casi in cui si omette la rimozione/disabilitazione, per trarre un eventuale maggior lucro dalla permanenza del file contestato come lesivo[60] o perché il soggetto leso è più "potente" e/o rinomato dello sconosciuto uploader.

Questo naturalmente non impedisce che il concorso sia regolato dall'articolo 2055, dal momento che –come detto- la disposizione regola il concorso di qualunque condotta, a prescindere dalla sua qualificazione in termini aquiliani o contrattuali, come viene comunemente ammesso.

4. L'ambito soggettivo di applicazione

La normativa specificamente dedicata a questo argomento è stata oggetto di armonizzazione europea ad opera della nota

[59] Del resto l'affermazione di Bocchini non è molto argomentata, limitandosi egli a scrivere che <<*onde se questa diligenza manca egli non rispodnerà –si ritgiene- a titolo di colpa, ma a titolo di dolo, inquanto l'inerzia successiva alla cosncenza di un fatto illecito comporta una responsabilità per dolo e non per colpa*>> (Bocchini F., *La responsabilità civile plurisoggettiva,,* cit., p. 2611).

[60] Nel diritto statunitense non c'è responsabilità per compartecipazione (*contributory infringement*) in tema di violazione di marchio, quando ricorra incertezza sull'estensione o sulla natura dell'attività contraffattoria: altrimenti verrebbe messo in pericolo il modello di business e-commerce, dato che questo verrebbe in pratica gravato di garantire l'autenticità delle merci ivi presenti. Pertanto c'è responsabilità solo se ricorre *willful blindness*: la quale può essere esclusa se il convenuto non sapeva dell'elevata probabilità di condotta illegale e [o, direi] volutamente ha fatto in modo di evitare di venirlo a sapere o di approfondire le indagini per paura dei risultati: cioè la *willful blindness* ricorre in caso di <<*bad-faith indifference to infringement*>> (Bruce Rice R.-Ho D., *Sound Policy and Practice in Applying Doctrines of Secondary Liability Under U.S. Copyright and Trademark Law to Online Trading Platforms: A Case Study*, in *Int. prop. & tech. law jour*., 2020/1, 7-8).

direttiva 31 dell'8 giugno 2000, recepita da noi con il decreto legislativo 70 del 9 aprile 2003 (di seguito: dir. 2000/31).

la disciplina sul punto specifico è posta dagli articoli 14-17 del d. lgs. cit.. Negli articoli 14-16 sono regolate tre figure di internet provider, mentre l'articolo 17 pone il divieto di assoggettare il provider ad un obbligo generale di sorveglianza (oltre ad altri precetti). Quest'ultimo divieto concerne tutte e tre le figure predette e si applica a prescindere dal fatto che beneficino o meno dell'esenzione di cui agli artt. 14-16[61]: basta che il tipo di attività svolta –quella considerata volta per volta, potendo egli svolgere più tipi di attività contestualmente- rientri nei concetti di access-mere conduit/caching/hosting. La Corte di Giustizia (di qui in poi: C.G.) ha precisato che un dovere di monitoraggio generale contrasterebbe pure con l'art. 3.1 della dir. 2004/48 (misure leali ed eque)[62]: il che allora lo estende a tutta la proprietà intellettuale (o quella regolata dalla dir. cit.), on line oppure offline[63], come sostanzialmente riaffermato poi in Tommy Hilfiger+5 c. Delta Center[64].

L'ambito soggettivo di applicazione degli artt. 14-17 è quello dei prestatori di un "servizio della società dell'informazione", che trova una definizione nell'art. 2 c. 1 lett. a): <<"servizi della società dell'informazione": le attività economiche svolte in linea -on line-, nonché' i servizi definiti dall'articolo 1, comma 1, lettera b), della legge 21 giugno 1986, n. 317, e successive

[61] Invece secondo M. Husovec, *Injunctions aganist intermediaries in the European Union. Accountable but not liable?*, Cambridge University Press 2017, 118, l'art. 15 dir. 31 presuppone che si applichino i safe harbours: ma il dettato non lo prevede affatto ed è lecito presumere che un così significativa regola avrebbe dovuto essere esplicitata.

[62] in *Scarlet Extended*, C-70/10, § 36.

[63] Secondo M. Husovec, *op. loc. ult. cit.*, ciò fa si che il divieto di monitoraggio A) ecceda l'applicabilità del safe harbour e cioè B) riguardi pure l'attività offline. Ma come appena detto alla nota 60, da un lato, B) non è conseguenza necessaria di A) e, dall'altro, A) era già ricavibile pianamente dalla disposizione europea. L'a. indica poi diversi precedenti, secondo cui il divieto di monitoraggio generale è affermato pure dalla Corte E.D.U. (ivi nota 40).

[64] C.G. 07.07.2016, C-494/15, §§ 30 e 36, riferito alla dir. 2004/48, art. 11 terza frase. Il divieto di monitoraggio è ricordato al § 34, ove si legge <<*Non si può neppure esigere che l'intermediario eserciti una vigilanza generale e permanente sui suoi clienti. Per contro, l'intermediario può essere costretto ad adottare provvedimenti che contribuiscano ad evitare che abbiano luogo nuove violazioni della stessa natura da parte dello stesso commerciante*>>: dunque senza menzionare l'art. 15 dir. 31.

modificazioni;>>[65]. La definizione della dir. 31/2000 (art. 2 lett. a), invece, avviene tramite rimando alla dir. 98/34 (modificata dalla dir. 98/48), il cui art. 1 punto 2 recita: << «servizio»: qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi. Ai fini della presente definizione si intende: — «a distanza»: un servizio fornito senza la presenza simultanea delle parti; — «per via elettronica»: un servizio inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento (compresa la compressione digitale) e di memorizzazione di dati, e che è interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici od altri mezzi elettromagnetici; — «a richiesta individuale di un destinatario di servizi »: un servizio fornito mediante trasmissione di dati su richiesta individuale>>. Il nostro requisito dell'<<economicità>> dell'attività voleva probabilmente recepire quello europeo della "prestazione normalmente dietro retribuzione" (il cons. 18 dir. 31/2000 parla di "attività economiche", anche se è da vedere la corrispondenza con l'uguale concetto interno). "Economicità" potrebbe –in prima battuta- interpretarsi come la teoria dell'imprenditore interpreta il riferimento all'attività economica, presente nell'art. 2082 cc[66] e cioè nel senso per cui non è necessario il fine di profitto, bastando il programmato pareggio dei costi (c.d. metodo economico): non potendosi ravvisare economicità –in breve-, se si deve programmaticamente (cioè ex ante) ricorrere

[65] Il c. 2 dell'art. 2 precisa: <<*L'ambito regolamentato comprende unicamente i requisiti riguardanti le attivita' in linea e non comprende i requisiti legali relativi a: (...) c) i servizi non prestati per via elettronica*>>. Dunque le due norme dell'art. 2 –ma anche il solo c.2- si rifeirscono a concetti diversi, una ai servizi on line e l'altra a quelli prestati in via elettronica, quasi che coincidano: il che non è, poiché un servizio può essere prestato in via elettronica ma non on line, mentre non è possibile –credo- il contrario (il servizio a distanza cartaceo non è *in linea -on line-*). La definizione della dir. unisce il requisito della via elettronica a quello della prestazione a distanza (v. il testo subito sotto), sicchè parrebbe più precisa: però dire come fa il ns. d. lgs. 70/2003 che si riferisce ai servizi prestati on line è sufficiente poiché già implica l'uso dello strumento elettronico, per cui è superflua l'esclusione dei servizi non prestati per via alettronica, i quali giammai potrebbero essere inclusi nel concetto di servizi *in linea -online-*.

[66] Anzi immagino che i redattori volessero proprio rifersi ad esso.

a sovvenzioni esterne per garantire la sostenibilità dell'attività[67]. Potrebbe però osservarsi che tale impostazione "nazionale" rischia di essere diversa dalla norma europea, la quale non solo non menziona il termine "impresa"[68], ma palesemente si disinteressa dell'adozione o meno (ex ante) del metodo economico: secondo la dir., infatti, basta che si tratti di un servizio, che la politica aziendale vuole "normalmente" retribuito, a prescindere dal suo ammontare e cioè dalla sua idoneità (ex ante, prospetticamente) a coprire quanto meno i costi. Pertanto il recepimento restringerebbe il concetto di "servizi della società dell'informazione" rispetto alla disposizione europea (richiedendo il metodo economico, che la dir. non prevede) e perciò ne restringerebbe l'ambito applicativo: con qualche problema di (in-)esatta attuazione nazionale. A parte ciò[69], il recepimento pare corretto (anche se

[67] Ex multis, v.: Spada P., voce *Impresa*, *Dig. disc. priv.-sez. comm.*, Utet, VII, 1992, p. 50 ss; Bonfante G.-Cottino G., *L?imprenditore*, in *Tratt. dir. comm.* dir. da Cottino, vol. I, Cedam, 2001, p. 415-417; Buonocore V., voce *Impresa (dir. priv.)*, in *Enc. dir*., Giuffrè, 2007, Annali, I, §§ 21 e 23; E. Desiana, *L'impresa fra tradizione e innovazione*, Giappichelli, 2018, 41 ss e 50-52. Il termine europeo "normalmente dietro retribuzione" andrà letto in base allo scopo della dir. di migliorare il mercato interno del commercio elettronico (conss. 1-4, 40). Viene allora da chiedersi perché sia stato inserito l'avverbio "normalmente" e cioè a quali ipotesi pensassero i redattori del testo: sarebbe stato più chiaro che la disciplina avesse riguardato solo i servizi prestati dietro retribuzione. La riflessione sull'economicità si interseca con quella sullo scopo di lucro (espressamente non previsto per l'impresa, ma solo per le società: art. 2247), a sua volta da distinguersi tra lucro soggettivo e lucro oggettivo.

[68] Concetto poi che –almeno a fini antrust- possiede un'ampia portata, dato che vale "attività economica", la quale come parrebbe comprendere pure le attività prive di fine di lucro. V. ad es.: Corte Giust. 29.11.2007, C-119/06, Commissione c. Repubblica Italiana, §§ 36- 37; Corte Giust. 10.01.2006, C-222/04, Ministero Economia e Finanze c. Cassa di Risparmio di Firenze s.p.a.+2, §§ 107-125 e spec. § 123. Nel § 107 di quest'ultima sentenza si legge l'inciso che si ritrova spessissimo nella giurisprudenza antitrust: <<*secondo costante giurisprudenza, nell'ambito del diritto della concorrenza il concetto di «impresa» comprende qualsiasi ente che eserciti un'attività economica, a prescindere dal suo status giuridico e dalle sue modalità di finanziamento*>>. Non è dunque chiarissimo il dire che la giurisprudenza europea nega la necessità dello scopo di lucro, ritenendo <<*sufficiente la semplice economicità di gestione*>> (Libertini M., *Diritto delle concorrenza dell'Unine Europea*, Giuffrè, 2014, 78)

[69] La mera richiesta di retribuzione, infatti, di per sé nulla dice sul rispetto o meno del metodo economico: dipende dal livello della retribuizione concretamente chiesta in relazione alla struttura dell'azienda e dei suoi costi. Bisognerebbe allora indagare il concetto usato dalla dir. per capire se basti una retribuzione di qualunque ammontare o invece se ne esiga una che almeno

qualche osservazione critica non sarebbe difficile da immaginare), tranne che per l'omesso riferimento all'avverbio "normalmente". Questo permette di includere nell'ambito applicativo della dir. anche i servizi che "talora" (cioè "non di norma") son forniti gratuitamente, rectius liberalmente[70]: possibilità che forse esiste anche nel recepimento nazionale, dato che possono pure essi venire compresi nel metodo economico, il quale appunto, non mirando al profitto, può fare varie scelte di business e cioè compensare operazioni profit con operazioni non profit[71], anziché solamente fissare ex ante una volta per tutte prezzi (sperabilmente) profittevoli.

Sia nel testo europeo che in quello italiano manca il riferimento a due elementi della definizione codicistica dell'imprenditore ex art. 2081: la professionalità e l'organizzazione, solitamente intesi il primo come sinonimo di abitualità o non sporadicità e il secondo come necessità di un minimo di eteroorganizzazione (l'attività del titolare non può essere l'unico elemento)[72]. Si deve prendere atto che non sono necessari: quello che conta è che l'interprete riesca a ravvisare la prestazione di un'attività economica o (secondo la

permetta di ravvisare il metodo economico. Come accennato, però, non ci sono elementi per pensarla nel secondo modo. Al legislatore europeo bastava, parrebbe, che non si trattasse di atto liberale.

[70] Quindi non solo le attività che singolarmente prese sono gratuite, ma che non sono liberali in quanto nella complessiva logica imprenditoriale sono finalizzate al profitto, soprattutto perché effettuate a fini promozionali (v. caso C.G. 15.09.2016, C-484/14, Mc Fadden c. Sony, §§ 41-42), ma anche quelle strettamente liberali (anche se per le imprese la distinzione non è semplice). Come detto pure nel testo, l'apparente gratuità di molti servizi internet non è tale, in quanto il corrispettivo è dato dalla cessione del diritto di usare i propri dati personali (tracciati dal prestatore, di solito la piattaforma): altrimenti, paradossalmente, le Big Tech Companies (di seguito solo "Big Tech") non potrebbero fruire del safe harbour perché rendono servizi non retribuiti! Va però ricordato che, pur essendo di solito inquadrate appunto come *tech companies*, in realtà sono *advertising companies and middlemen in the flow of information*: Google e Facebook traggono dalla pubblicità rispettivamente l'80 e il 98 % delle loro entrate (Stoller M., *Spotify Is Mimicking Google's and Facebook's Strategy: Will It Ruin Podcasting?*, promarket.org, 06.03.2020); entrambe il 90 % per Woodcock R.A., *The Obsolescence of Advertising in the Information Age*,Yale Law Journal, 2018, vol. 127, 2272.

[71] Si pensi al tipo di attività svolta oggi dalle società benefit ex L. n.208 del 28/12/2015 (legge di Stabilità 2016) art.1, c. 376-384.

[72] Cetra A., *La nozione di impresa*, in Cian a cura di *Diritto commerciaale*, Giappichelli, I, 2013, p. 33-35.

disposizione europea) di un servizio, fermi gli altri requisiti della fattispecie[73].

5. Si tratta di disciplina in negativo (esenzione da responsabilità), non affermativa di responsabilità

Le tre figure di provider sono regolate non in positivo, bensì in negativo. Non si dice infatti quando sono responsabili, bensì si delimita un'area, in cui non possono essere ritenuti responsabili: area costituita dal rispetto delle condizioni ivi fissate[74]. La formulazione sia del testo italiano sia della direttiva

[73] Si potrebbe anche dire che –astrattamente- il concetto di "attività" non equivale a quello di "servizio": il secondo può teoricamente svolgersi anche una sola volta (*societas unius negotii*), mentre l'attività si riferisce ad un fenomeno sociale più complesso o strutturato, presupponendo una plurlaità di atti coordinati ad un fine. Potrebbe però replicarsi che ciò vale per il diritto nazionale o anzi che il concetto di servizio nelle direttive citt. equivale grosso modo al nostro di attività.

[74] Gli studi più attenti sono abbastanza concordi: v. Piraino F., *Spunti per una rilettura dela disciplina giuridica degli internet service provider*, AIDA XXVI-2017, 468 ss, 472-473; Montagnani M.L., *Internet, contenuti illeciti e responsabilità degli intermediari*, Egea, 2018, 49; Nordemann J.B., *Liability of online service providers for copyrighted content-Regulatory action needed?*, gennaio 2018, p. 8 e 21 (studio eseguito su incarico del Parlamento Europeo): l'a. propone l'introduzione di una disciplina in postivo della responsabilità civile per gli internet service provider, p. 25; Shikhiashvili L., *The same problem, different outcome: online copyright infringement and intermediary liability under US and EU laws*, in *Intell. prop. & tech. L.J.*, 2020, vol. 24, 147.; negli USA, Bruce Rice R.-Ho D., *Sound Policy and Practice in Applying Doctrines of Secondary Liability*, cit., 6; Sag M., *Internet Safe Harbors and the Transformation of Copyright Law*, in *Notre Dame Law review*, 2017, vol. 93/2, 499 ss, 512-513 (tuttavia le condizioni per il safe harbour del DMCA costituscono un *de facto standard* per le piattaforme: p. 513-514); evitano gli effetti di una *prima facie liability* per Riordan J., *The liability of internet intermediaries*, cit., p. 379, sub 12.11, e p. 384 sub 12.35. Contrario R. Bocchini, *La responsabilità civile degli intermediari del commercio elettronico. Contributo allo studio dell'illecito plurisoggettivo permanente*, ESI, 2003, p. 123-124; contrario pure De Cata M., *La responsabilità civile dell'internet service provider*, Giuffrè, 2010, p. 199 per il quale "*Le esenzioni da responsabilità tuttavia non hanno solo sottratto dall'ambito di applicazione della sanzione determinati comportamenti omissivi, ma vi hanno altresì ricompreso determinate condotte negative. Infatti, benché formulate come condizioni negative, le exemptions non stabiliscono l'irresponsabilità del provider in alcuni casi tassativamente previsti, ma, al contrario, sanciscono In tali casi la responsabilità del prestatore di servizi. Infatti le exemptions non escludono la sanzione per comportamenti positivi ma prevedono la responsabilità per condotte negative*". Non vedo però come si possa sostenere ciò, alla luce del dettato legislativo. Non distinguono tra esenzione ed affermazione di responsabilità nella dir. 2000/31 Martinelli S., *L'autorità privata del provider*, in Sirena-Zoppini (a cura di), *I poteri privati e il diritto della regolazione, A quarant'anni da <<Le autorità private>> di C.M. Bianca*, Roma

è univoco in questo senso, laddove così recita: "Nella prestazione del servizio … il prestatore non è responsabile delle informazioni trasmesse/della memorizzazione/delle informazioni memorizzate.. a condizione che:.." (così l'incipit degli art. 14-16 e analogamente nella dir.). Pertanto, una volta esclusa l'applicabilità delle esimenti specifiche, non è detto che il provider diventi automaticamente responsabile o –meglio- che abbia agito in violazione (la responsabilità sorge solo in presenza di danni provati e causalmente ricollegabili): la sua posizione, infatti, andrà scrutinata in base alla disciplina comune, la quale potrebbe -ad es. e almeno in linea teorica- permettere di invocare qualche esimente generica (adempimento di dovere, stato di necessità, consenso dell'avente diritto etc.)[75].

Su questo profilo sorvola certa giurisprudenza, ad es. quando, con poca precisione, dopo aver rilevato che il d. lgs. 70/2003, pur se non applicabile a Wikipedia perché stabilita in paese non appartenente allo S.E.E. (art.1 c.2 lett. d)[76], tuttavia contiene "*le necessarie direttrici giuridiche di riferimento per l'inquadramento della fattispecie. Analogamente e conformemente pertanto a quanto previsto negli artt. 16 e 17 del D. L.vo 70/2003 e sulla base dell'elaborazione giurisprudenziale formatasi sul tema (…), la responsabilità dell'Internet Service Provider deve ritenersi sussistente per le informazioni oggetto di hosting (memorizzazione durevole) soltanto allorquando il provider sia effettivamente venuto a conoscenza del fatto che l'informazione è illecita e non si sia attivato per impedire l'ulteriore diffusione della stessa e ciò in assenza di un generale obbligo di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite, né potendo ritenersi integrata alcuna posizione di garanzia, in*

Tre-Press, 2018, p. 565 (per di più affermando un concetto originale di <provider attivo>: quello che di fatto esegue controlli sui file ospitati, senza rimuovere quelli illeciti) né Bussani M., *L'illecito civile*, cit., 849 (l'armonizzazione UE ha <<precisato le condizioni per la responsabilità (e l'immunità) dei gestori degli internet providers (direttiva 2000/31/CE")>>). Pare scambiare l'esenzione da responsabilità con l'ascrizione della stessa anche Gqambini M., *La responsabilità dell'internet service provider approda al vaglio della Cassazione*, nota a Cass. 7708 e 7709 del 19.03.2019, in *Il corr. giur*., 2020/2, p.188.

[75] Seminara, S. voce *Internet (diritto penale)*, *Enc. dir., Annali*, Giuffrè, 2014, 592-3, per la responsabilità penale.

[76] Per la precisione la Corte rileva che così era stato affermato dal Tribunale senza contestazioni dalle parti.

assenza di norme che radichino la responsabilità oggettiva o di posizione del provider o l'esistenza in capo allo stesso di un obbligo di controllo"[77]. La sentenza dunque da un lato estende per analogia la regola di matrice europea ad un provider, che non vi è soggetto, e dall'altro fa dir loro più di quel che in realtà dicono. Infatti fa intendere che il requisito (assenza di conoscenza o pronta rimozione), che nella prima è posto in positivo e cioè per fruire del safe harbour, viene qui usato in negativo e cioè per ravvisare l'illecito, nel senso che, quando non ricorre (perché il provider sa e non agisce), questi sarà per ciò solo responsabile.

La natura di norme, che si limitano ad escludere l'illiceità, come si è accennato, vale in teoria. In pratica, sarà improbabile che la non fruibilità del safe harbour porti ad un giudizio di liceità della condotta del provider: le condotte menzionate per il safe harbour, infatti, costituiscono –in generale[78]- anche concretizzazione di diligenza, per cui non adottarle costituirà

[77] App. Roma n. 1065/2018 del 19.02.2018, Rg 4312/2013, *Cesare Previti c. Wikimedia* (su presunti errori nella relativa voce di Wikipedia), p. 9-10

[78] Il discorso andrebbe articolato per ciascuna condizione di esenzione, ma parrebbe esatto che il non rispettarle costituisse in linea di massima negligenza cioè colpa ex art. 2043-2055 (ad es. modificare le informazioni, in forma di partecipazione diretta –commissiva-; il ritardare la rimozione/disabilitazione, in forma omissiva).

spesso negligenza[79]. Altra dottrina concorda sul punto[80].

6. Le tre figure tipizzate e il problema della pretesa passività del provider

Le figure considerate sono quelle: i) del provider che svolge attività di semplice trasporto (o di fornitura di accesso alla rete), ii) del provider che svolge un'attività di memorizzazione solo temporanea; iii) del provider che svolge un'attività di memorizzazione permanente, cosiddetto hosting provider.

In generale -nel senso che il principio vale per qualunque tipo di provider- l'esimente (deroghe alla responsabilità) opera quando il ruolo del provider è solo "tecnico automatico e passivo" (cons. 42 dir. 31/2000): così almeno si legge spesso.

[79] C'è però già un'applicazione dell'esito, sopra ritenuto improbabile, di un'esclusione sia del safe harbour sia di responsabilità. Trib. MI 09.09.2011 (primo grado del processo poi conclusosi –per ora- con Casss. 7708/2019, RTI c. Yahoo), AIDA, 2012, § 1505, p. 748, § 4., non concede il safe harbour a Yahoo per la sezione Video del suo portale, ma rigetta la domadna in termini di responsabilità civile generale, rilevando "*l' impossibilità anche per il prestatore di servizi che fornisca hosting attivo di potere procedere ad una verifica prventiva del materiale immesso quotidianamaente dagli utenti, non potendosi ritenere tale verifica quale comportamento effettivamente esigibile per la sua (àttuale) complessità tecnica che un controllo del genere richiederebbe anche in relazione ai possibili conflitti di forme di controllo automatico -che sembrano le sole apparentemente attuabili a fronte della mole di materiale da esaminare- con forme di libera manifestazione del pensiero o di utilizzazione di contenuti protetti dal diritto d'autore per i quali possa fondatamente richiamarsi una delle ipotesi di utilizzazione libera*" (ivi). Solo che nega il safe harbour speciale sull'aprioristico giudizio di non concedibilità dello stesso, quando si tratti di hosting attivo: non si confronta però col fatto che il contenuto del cons. 42, da un lato, non è ripetuto nell'articolato e, dall'altro, è comunque riferito solo all'access e al caching provider (punto svolto oltre nel testo). Sul fatto che i requisiti del safe harbour influenzino anche la responsabilità in positivo concorda Montagnani M.L., *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., 50, 60, 71-2. Astrattamente però la disciplina dell'esonero e quella in assenza di esonero sono separate, dato che, se non è invocabile, potrebbe esserci ancora spazio per un giudizio di liceità: è solo in via fattuale che tende a profilarsi l'alternativa <esonero da safe harbour/violazione> (non chiara sul punto Montagnani M.L., *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., 87).

[80] Simile osservazione in Bravo F., voce *Commercio elettronico*, cit., 309/310. La distinzione tra esenzione da responsabilità e affermazione di responsabilità è netta in Cotropia C.A.-Gibson J., *Convergence and Conflation in Online Copyright*, in *Iowa law review*, 2020, vol. 105, 1029-1030 e 10447-1048: gli aa. lamentano però che anche là le Corti hanno inizialmente utilizzato gli standard della prima (§ 512 DMCA) per giudicare sulla seconda (liability in common law) (v. sub III, 1049 ss), per poi giungere a confonderle (v. sub IV, 1066 ss).

Vale la pena di soffermarvisi, dato che tocca una delle questioni più dibattute nelle aule giudiziarie: e del resto è solo qui che la dir. adopera l'aggettivo "passivo", cui viene poi data grande importanza da parte della giurisprudenza e dottrina italiana[81], per riassumere le caratteristiche dei provider necessarie per fruire delle esimenti.

Ebbene secondo il cons. 42), <<*le deroghe alla responsabilità stabilita nella presente direttiva riguardano esclusivamente il caso in cui l'attività di prestatore di servizi della società dell'informazione si limiti al processo tecnico di attivare e fornire accesso ad una rete di comunicazione sulla quale sono trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi al solo scopo di rendere più efficiente la trasmissione. Siffatta attività è di ordine meramente tecnico, automatico e passivo, il che implica che il prestatore di servizi della società dell'informazione non conosce né controlla le informazioni trasmesse o memorizzate.*>>. La "disposizione"

[81] Per tutti v. i tre recenti lavori di Tosi E.: - *Obblighi di filtraggio ex post di contenuti digitali illeciti equivalenti e responsabilità civile dgli hosting provider*, in *Il dir. ind*., 2020/3, 287-294 (si tratta di nota -sostanzialmente favorevole: p. 298- a C.G. 03.10.2019, C-18/18, Eva Glawischnig-Piesczek c. Facebook); - *La disciplina applicabile all'hosting provider per la pubblicazione di contenuti digitali protetti dal diritto di autore, tra speciale irresponsablità dell'ISP passivo e comune responsabilità dell'ISP attivo, alla luce di Cassazione 7708/2019 e 7709/2019*, nota a Cass. 21.03.2019 n. 7708 e 7709, in *Riv. dir. ind*., 2019/4-5, 226 ss, passim; - *L'evoluzione della responsabilità civile dell'0internet service provider passivo e attivo, Il dir. ind*., 2019/6, 590 ss. Non segue l'accezione giurisprudenziale del concetto di provider <attivo> (e per esclusione, <passivo>) Tescaro M., *Una proposta ricostruttiva contrastante con il diritto vivente in tema di responsabilità civile dell'internet provider nel diritto italiano tra direttiva 2000/31/CE, regolamento UE 2016/679 e direttiva UE 2019/790*, in *juscivile.it*, 2020, 62 ss.: per questo a., <attivo> è il provider che: 1) fornisce direttamente contenuti; oppure ii) esercita autorità o controllo sull'attività dell'utente, nel quale caso l'art. 14 § 2 dir. 2000/31 (art. 16 c. 2 d. lgs. 70/2003) esclude che si applichino i presuppposti di responsabilità previsti per il provider passivo (p. 68/9). Ora, a parte che, da un lato, l'art. 14 § 2 d. lgs. 70/2003 nel caso dell'<autorità e controllo> esclude il safe harbour, invece che la responsabilità, e, dall'altro, è scontato che non benefici di safe harbour il provder che sia l'autore dei contenuti o dell'uploading (la fattispecie legale concerne il caso di <memorizzazione di informazioni fornite da un destinatario del servizio> e non dal prestatore del servizio, quale è il provider), il vero problema è proprio capire quando ricorra <autorità o controllo> sull'attività dell'uploader: in particolare se ricorra in base alla sola attività di indicizzazione e promozione dei contenuti caricati dagli utenti e/o in base alle clausole contrattuali fatte sottoscrivere a questi ultimi (v. quanto osservato sul punto in questa parte del testo).

(se può parlarsi di disposizione per un precetto che figura solo in un considerando) è comprensibile: nel triplice conflitto di interessi considerato dal legislatore (diritto di espressione, di informazione e di essere informati; diritto di impresa del provider; diritto all'onore o di IP, incluso il right of publicity[82], di chi può venir leso dalla attività on line altrui)[83], l'esenzione da responsabilità per questa industria –a quel tempo allo stato quasi nascente[84]- ha senso solo se i provider non influiscono sui

[82] Lamenta la violazione frequente sui social media del *right of publicity*, anche perché manca una legge federale e non tutti gli Stati ne hanno adottato una loro (anzi, solo meno della metà: ventidue, p. 36), Carr N. K., *Social Media and the Internet Drive the Need for a Federal Statute toProtect the Commercial Value of Identity*, in *Tulane Journal of Technology andIntellectual Property*, 22, 2020, p. 31 ss. (auspicando appunto l'introduzione di legge federale per le difficoltà di pianificare la gestione di questo bene, a tutela non solo delle c.d. celebrità, p. 40 ss e 47 ss.).

[83] Nel caso C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, mentre le conclusioni dell'AG avevano segnalato la rilevanza pure dell'eisgenza di rispettare la libertà di espressione (§ 65), la sentenza la dimentica (nel senso che non ne parla, se non riportando in virgolettato qualche considerando della dir. 31/2000) e menziona solo libertà di impresa del provider e diritto all'onore/reputazione del soggetto leso (§§ 43-44): cosa assai sorprendente, anche perché la libertà di espressione è espressamente garantita dalla Carta dei diritti fondamentali dell'UE, c.d. Carta di Nizza, (inizialmente approvata il) 07.12.2000, che ora ha lo stesso valore dei Trattati ex art. 6 TUE). Lo rileva pure Monti M., *La Corte di giustizia, la direttiva e-commerce e il controllo contenutistico online: le implicazioni della decisione C 18-18 sul discorso pubblico online e sul ruolo di Facebook*, 15.10.2019, medialaws.eu, § 4.

[84] La protezione delle imprese nei settori nuovi, in termini di cautela nell'aggiudicare responsabilità, è una costante, evolvendosi poi la disciplina verso un aggravamento delle responsabilità quando il settore è maturo ed è stato meglio soppesato il rapporto tra costi e benefici: v Bocchini R., *La responsabilità di Facebook per la macnata rimozione di contenuti illeciti*, nota a Trib. Napoli nord, 03.11.2016, Facebook c. T.G., in *Giur.it.*, 2018/3, 636; Castronovo C., *La responsabilità civile*, cit., p. 439-440; spunti storici sulla regolamentazione dell'innovazione tecnologica in Black J.-Murray A.D., *Regulating AI and Machine Learning: Setting the Regulatory Agenda*, in *Eur. J. of law and tech.*, 2019, vol. 10/3, §§ 1-2 e § 3 sulle prospettive per intelligenza artificiale (di seguito solo A.I.) e Machine learning. Per questo motivo l'esenzione totale dei provider ex § 230 CDA ha perso ragionevolezza (Gabison G.-Buiten M.C., *Platform liability in copyright enforcement*, in *Columbia Science & technology law review*, vol. XXI, spring 2020, 243 e 278/9, saggio centrato sul rapporto tra piattaforme e copyright): è dunque oggi opportuno affermare la responsabilità delle piattaforme, dato che: i) beneficiando del traffico sui loro siti, è giusto che internalizzino le perdite che in tal modo causano a terzi, ii) come *potential least cost avoiders*, tocca a loro il peso dell'enforcement, secondo la nota regola di efficienza; iii) la responsabilità le indurrebbe ad investire sempre più in sistemi di filtraggio automatico; iv) indurrebbe le piattaforme a stipulare contratti di licenza con i

contenuti e si limitano a fornire un servizio tecnico. Incredibilmente l'indagine, condotta dall'US Copyright Office sull'applicazione del § 512 DMCA e conclusasi nel maggio 2020, considera solo gli ultimi due interessi e dimentica il primo (quello della collettività ad esprimersi e ad essere informata)[85].

titolari dei diritti, verso cui non hanno inventivi in caso di safe harbour totale (*op. ult. cit.*, sub III, 247 ss.). Può essere allora che anche il safe harbour ex dir. 2000/31 verrà ridotto col passar del tempo e si parla ormai diffusamente della possibilità di revoca di quello offerto in USA dal § 230 del Decency Act: così ad es. Joe Biden nell'articolo di C. Lima, *Biden: Tech's liability shield 'should be revoked' immediately*, in politico.com del 17.01.2020 che riferisce –probabilmente- della lunga intervista condotta dal New York Times realizzata il 16.12.2019 e pubblicata pure il 17.01.2020; anche se i più virulenti attacchi provengono da parte repubblicana, che ritiene sé stessa maggiormente danneggiata dalla *content moderation* praticata dalle piattaforme e soprattutto da Facebook (Weintraub E. L.-Moore T.H., *Section 230*, in *Georgetown technology law review*, vol. 4.2, 2020, 628, i quali propongono di gravare le piattaforme di un tributo per l'esternalità negativa da esse creata, consistente nel danno prodotto al processo democratico, p. 635 ss.; Vogels E.A.-Perrin A.-Anderson M., *Most Americans Think Social Media Sites Censor Political Viewpoints*, 19.08.2020, *Pew Resarch Center*). Accenna ad un possibile venir meno dell'iniziale ratio del safe harbour l'AG Saugmandsgaard ØE in C.G., C-682/18 e C-683/18, Peterson c. Google-Youtube e Eelsevier c. Cyando, §§ 245-246; dettagliate racomandazioni per la disciplina della moderazione dei contenuti nell'ampio studio di Harold Feld, *The Case for the Digital Platform Act: Market Structure and Regulation of Digital Platforms*, maggio 2019, cap. V e soprattutto V.D, p. 149 ss (v. pure V.C, p. 138 ss, sul § 230 CDA); ne sostiene invece la permanente utilità Matula C., *Any Safe Harbor in a Storm: SESTA-FOSTA and the Future of § 230 of the Communications Decency Act*, in *Duke Law & Technology Review*, vol. 18, 2020, p. 353 ss, passim, richiamandone l'utilità e quindi la necessità di attenta ponderazione in caso di modifiche (sub IV; a p. 361 l'a. osserva che gli elevati costi di compliance alla legge c.d. SESTA-FOSTA, che deroga al safe harbour, hanno indotto le grandi piattaforme ad appoggiare l'iter legislativo, in quanto solo loro potranno sopportarli; le istanze contrarie al mantenimento del § 230 CDA provengono dai giudici, p. 363 ss, e dai politici, p. 365 ss)

[85] <<*The sharp divergence in the assessments of section 512 by OSPs and copyright owners indicates that the statute in practice is not achieving the balance Congress originally intended. While this divided opinion by itself is not conclusive, the fact that one of the two principal groups whose interests Congress sought to balance is virtually uniform in its dissatisfaction with the current system suggests that at least some of the statute's objectives are not being met*.>> (v. il *Section 512 of title 17. A report of the Register of Copyright, May 2020*, (v. sub V.B.3, p. 83).. Dunque non solo non mette gli interessi del pubblico tra i principali che il legislatore cercò di bilanciare, ma nemmeno li menziona tra quelli non principali. Va allora condivisa l'osservazione di Samuelson P., *The US Copyright Office Section 512 Study: Why the Entertainment Industry Is Claiming Victory*, 25.05.2020, in *kluweriplaw.com*. In generale, secondo il Report l'evoluzione tecnologica a giuriprudenziale ha portato ad una eccessiva protezione delle piattaforme e ad una ridotta protezione dei titolari di copyright (Rechardt L.,

Questa precisazione è spesso utilizzata per escludere il safe harbor per quegli hosting providers, i quali svolgono attività, che i giudici ritengono eccedere quella di ruolo automatico e passivo: in particolare perché indicizzano, organizzano e promuovono i materiali caricati dagli utenti proponendoli ad altri navigatori[86] allo scopo di trarre profitto[87], soprattutto in

Balance lost: the US Copyright Office finds US copyright safe harbour provisions have been tilted askew, in *Journal of Intellectual Property Law & Practice*, Vol. 15/8, 2020, p. 571) Bene invece le Conclusioni dell'§AG Saugmandsgaard ØE in C.G., C-682/18 e C-683/18, Peterson c. Google-Youtube e Eelsevier c. Cyando, §§ 241-242, richiamando C.G. 16.02.2012, C-360/10, *Sabam c. Netlog*, § 44 segg.

[86] Si pensi a Cass. 19.03.2018 n. 7708 nella lite *RTI c. Yahoo*, § 4 e relativi sottoparagrafi, che la pensa all'opposto della decisione di appello, pur non cassandola, perché nel caso de quo non ravvisa gli estremi del provider attivo (§ 4.4).

[87] Più l'utente è attirato dalle proposte targetizzate o customizzate (mi si passi i due bruttissimi termine; "su misura", potremmo meglio dire), più resta nel sito e dunque più è esposto all'*advertising*, vera fonte di lucro delle piattaforme. Una breve ma chiara esposizione delle possibilità, offerte oggi alle campagne pubblicitarie dal microtargeting, trovi in Kotler Ph-Hollensen S,-Prensik M.O., *Social media marketing. Marketer nella rivoluzione digitale*, Hoepli, 2019 (orig.: 2019), p. 85-87. Per qualche altro cenno sul tema v. infra. E' stato poi giustamente osservato che il livello di elevata personalizzazione del microtargeting (scrive di "contenuti sminuzzati in *quanti* informativi difficili da controllare" Talia D., *La società calcolabile e i big data*, Rubbettino, 2018, 95 e 97) produce almeno due conseguenze di rilievo [in realtà diverse altre, credo, tutte da indagare]: i) permettendo di inviare certi contenuti (ad es. politici) solo a chi presumibilmente li condividerà, evita di farlo a chi invece probabilmente li rifiuterebbe; ii) sfugge a controlli e a fact-checking (Da Empoli G., *Gli ingegneri del caos. Teoria e tecnica dell'Internazionale populista*, Marsilio, 2019, 46). Per non dire che tale personalizzazione potrebbe radicalmente escludere i social dal *public discourse* e quindi dal Primo Emendamento, proprio venendo meno il lato "pubblico" (Grafanaki S., *Platforms, the First Amendment and Online Speech: Regulating the Filters*, 39 *Pace L. Rev.* 111 (2018), 131 w 151 ss): posizione non errata, se si considera che ad es. in materia di propaganda politica <<*consente alla forza politica, al candidato o ad altri soggetti comunque a ciò interessati di confezionare il messaggio su misura per il suo destinatario, escludendo tutti gli altri possibili destinatari, persino inviando messaggi contraddittori e di contenuto opposto ai diversi destinatari selezionati, con nessuna (o scarsa) probabilità che i vari soggetti possano venire a conoscenza dei messaggi inviati agli altri*>> (Grandinetti O., *La par condicio al tempo dei social, tra problemi "vecchi" e "nuovi" ma, per ora, tutti attuali*, in *Riv. dir. media*, 2019/3, medialws.eu, p. 117). Sul punto v. Hindman M., *La trappola di internet*, cit., cap. 3, p. 49 ss. Alla personalizzazione/targettizzazione del diritto (privato patrimoniale) è dedicato il fascicolo vol 86/2 (aprile 2019) della *The University of Chicago Law Review*, ove il saggio Gillis T.B.-Spiess J.L., *Big Data and Discrimination*, cit. infra: si v. quello che parrebbe il saggio introduttivo Casey A.J.-Niblett A., *A Framework for the New Personalization of Law*, ivi, 333. Il che rende possibile allora pure la *price discrimination*, sollevando problemi nuovi per la indesiderabilità dello

tema di violazioni di diritto d'autore[88]. Se però si legge con attenzione il cons. 42, la plausibilità dell'esposto ragionamento appare non poco incerta. E' vero che il suo incipit sembra riguardare tutte le esenzioni poste dalla direttiva e cioè tutti e tre i tipi di internet provider. Successivamente, però, il primo periodo del cons. si riferisce solo all'access-mere conduit e al caching, mentre non vi rientra l'hosting provider[89]. L'espressione <<*processo tecnico di attivare e fornire accesso ad una rete di comunicazione sulla quale sono trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi al solo scopo di rendere più efficiente la trasmissione*>>, infatti, è difficilmente -molto difficilmente- riferibile alla memorizzazione duratura, tipica dell'hosting provider. Del resto l'incipit del cons. 42 afferma senza mezzi termini che è <<esclusivamente>> in tali casi che i provider possono fruire del safe harbor posto della direttiva stessa: per cui l'hosting, sotto un profilo letterale, sarebbe escluso dal safe harbour. Inoltre il secondo periodo, contenente la famosa espressione "Siffatta attività è di ordine meramente tecnico, automatico e passivo", si riferisce appunto a "siffatta attività" e cioè a quella indicata nel primo periodo, il quale, come appena detto, non include l'hosting provider. In breve, il cons. 42 si

sfruttamento della *willingness to pay* (WTP) del consumatore, quando basata su erronee credenze (*misperceptoins*, o manipolazioni, aggingo): così Bar-Gill O., *Algorithmic Price Discrimination When Demand Is a Function of Both Preferences and (Mis)perceptions*, in *The University of Chicago Law Review*, vol. 86/ 2, 2019, che suggerisce interventi regolatori (v. soprattutto p. 228 ss e 242 ss). Nel diritto UE si v. sul tema Sears A.M., *The limits of online price discrimination in Europe*, in C*colum. Sci. & tech. L. Rev.*, 2019, vol. 21: l'a. esamina i possibili strumenti per contrastare la *online price discrimination* (antitrust, disciplina consumeristica, data protection; disciplina antidiscriminatoria) e conclude che l'ultimo è quello più proficuamente utilizzabile (p. 27 ss e 37). Vigorosa difesa dell'utilità, anche deterrente (p. 30 ss.), degli scorpori antitrust in Van Loo R., *In Defense of Breakups: Administering a "Radical" Remedy*, di prossima pubblicazione in *Cornell Law Review*, 2020, letto in ssrn.com (l'a. valorizza le positività dell'asseritamente analogo caso degli scorpori volontari, cioè non subiti ma voluti dagli organi di governance, sub III, p.20 ss.)

[88] Il ruolo propositivo può però teoricamente applicarsi anche per altre violazioni di proprietà intellettuale e pure di diritti della persona (promozione di audiovisivo diffamante etc.).

[89] Accenna ad un'idea simile Montagnani M.L., *Internet, contenuti illeciti*, cit., 95-96, anche se poi pare aderire all'estensione della "regola" all'hosting provider praticata dalla C.G..

riferisce ad access-mere conduit e a caching provider, non all'hosting provider[90].

Tuttavia poi l'articolato prevede all'articolo 14 appunto la figura dell'hosting provider: sembra quasi che quest'ultima tipologia sia stata aggiunta in un momento successivo, rispetto ad una prima redazione che non l'includeva, senza aggiornare il

[90] Profilo già rilevato da altri: - App, Milano 07.01.2015 n. 29, *Yahoo c. RTI*, RG 3821/2011, § 27 (il ricorso contro la quale è poi deciso da Cass. 7708/2019); - l'AG JÄÄSKINEN 09.12.2009, nel caso *L'Oreal e altri c. eBay*, C-324/09, § 141-142; Bugiolacchi L., *Evoluzione dei servizi di hosting provider, conseguenze sul regime di responsabilità e limiti dell'attuale approccio case by case*, nota a Trib. Milano 25.05.2013, ord., sez. I., rel. Miccicchè, in *Resp. civ. prev*., 2013, 2006/7; - Colaruotolo A., *Facebook e hyperlinking illecito degli utenti. L'inerzia ingiustificata del prestatore di servizi è fonte di responsabilità civile e risarcitoria*, nota a Trib. Roma 15.02.2019, *RTI c. Facebook-Ponzone*, in *Riv. dir. ind.*, 2019/4-5, 328. Ipotizzano un'errata lettura del cons. 42 pure Bridy A., *The Price of Closing the "Value Gap": How the Music Industry Hacked EU Copyright Reform*, in *Vand. j. ent. & tech. l.*, 2020, vol. 22/2, 337, e Riordan J., *The Liability of Internet Intermediaries*, OUP, 2016, 402, § 12.119). Non si cura di questo ostacolo chi segue la giurisprudenza sulla categoria concettuale dell'hosting attivo proprio appoggiandosi al cons. 42 (G. D'Alfonso, *Verso una maggiore responsabilizzazione dell' hosting provider tra interpretazione evolutiva della disciplina vigente, innovazioni legislative e prospettive de jure condendo*, in *Federalismi.it*, 2020/2, 22.01.2020, p.124/5, oltre che all'irrazionalità dell'equiparare operatori intrinsecamente diversi). Sarebbe però interessante approfondire quanto siano realmente diversi *in parte qua* i principali operatori al centro del dibattito mondiale, dato che tutti presentano i risultati –newsfeed di notizie o risutati di query- e l'offerta complessiva in modo da guadagnare il più possibile e in particolare base ad algoritmo costantemente modificato, per cui neutralità e passività non esistono sul web (come detto poi nel testo). Il quale tiene conto di molti fattori, tra cui la navigazione compiuta dall'utente e così pure la correlata offerta pubblicitaria, sicchè i prezzi variano diacronicamente e sincronicametne (cioè da soggetto a soggetto) pure in base alla storia di acquisti tracciata per ciascun utente, per cui addirittura rischia di venir meno –spt. nel diritto antitrust- il concetto di mercato come incontro aggregato di domanda e offerta e di "prezzo di mercato": così anche, mi pare, A. Mastrorilli, *Algoritrmo scellerato?*, *Merc. concorr. regole*, 2019, 2, 349; Sunstein C.R., *#Republic.com. La democrazia nell'epoca dei social media*, Mulino, 2017, p. 11 ss., scrive del "Daily Me" a proposito della personalizzazione dei Newsfeed informativi, riprendendo un termine creato da Nicholas Negroponte); Quintarelli S., *Capitalismo immateriale. Le tecnologie digitali e il nuovo conflitto sociale*, Bollati Boringhieri, 2019, 48-49. Addirittura le istruzioni informatiche (manco a dirlo!) possono essere concordate, per cui già si parla di *algorithmic cartels*: Lamontanaro A., *Bounty Hunters For Algorithmic Cartels: An Old Solution for a New Problem*, 30 *FordhamIntell. Prop. Media &Ent. L.J.* 1259 (2020), riferito ad accordi sulla fissazione di prezzi.

considerando[91].

In altre parole il cons. 42 dice cose assai diverse da quelle dette in parte qua dall'art. 14: non può dunque ravvisarsi nel primo una mera precisazione o esemplificazione della regola posta dal secondo. Il cons. 42 non può dunque riferirsi all'art. 14, dato che altrimenti le regole previste nel primo avrebbero dovuto essere riprodotte in qualche modo (anche se non negli stessi esatti termini, ma in modo inequivoco) nel secondo. In un caso come questo può insomma operare il brocardo *ubi lex voluit dixit, ubi noluit tacuit*: è infatti secondo ragione pretendere che una così importante regola, come quella dei requisiti menzionati dal cons. 42, sia presente anche nell'articolato, senza essere lasciata nel limbo dei considerando. Il che può dirsi allora per il recepimento nazionale: anche il d. lgs. 70/2003 si è astenuto dall'introdurla per l'hosting nell'art. 16 (possiamo applicare il predetto brocardo al quadrato!). Ebbene, se in due occasioni di normazione i requisiti, di cui al considerando, non sono entrati nell'articolato (né europeo, né nazionale), allora significa che non sono stati voluti.

Resta allora da capire meglio la portata del considerando 42, se si concorda che sotto il profilo letterale non si riferisce all'hosting provider[92].

---

[91] Secondo Petruso R., *La responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a confronto*, Giappichelli, 2019, 140, è successo proprio qualcosa del genere nell'iter legislativo: l'a. si riferisce all'originaria proposta della Commissione, della quale però non vengono purtroppo formiti dati identificativi né URL per accesso diretto. La proposta di direttiva 23.12.1998 (n° 1999/C 30/04 - COM(1998) 586 def. - 98/0325(COD)), che nella sezione Procedimento 1998/0325/COD del database legislativo parrebbe quella originaria, non supporta tale affermazione.

[92] Sotto questo profilo è poco persuasiva la sentenza di primo grado (nel processo poi deciso da Cass. 7708/2019), laddove, da un lato, riconosce che l'hosting provider non rientra nel cons. 42, e, dall'altro, dice che Yahoo è hosting provider ma non può fruire del safe harbour, dato che la sua ricca attività di catalogazione/indiciazzione etc. non permette di considerarlo "passivo" (Trib. Milano 09.09.2011 n. 10893, RTI c. Yahoo, in Pluris on line, § 4). Trascura infatti il Tribunale di reperire base normativa a detto requisito di passività; né può essre reperito nella giurisprudenza europea, la quale pure non si pone il problema e del resto è vincolante solo per il giudice a quo (anche se la dottrina sostiene un'estensione più ampia, oltre il caso specifico, quasi uno *stare decisis* di common law: - Strozzi G.-Mastroianni R., *Diritto dell'Unione Europea. Parte istituzionale*, 8 ed., Giappichelli, 2019, p. 447/8; - Tesauro G., *Sui vincoli (talvolta ignorati) del giudice nazionale prima e dopo il rinvio pregiudiziale: una riflessione sul caso Avastin/Lucentis e non solo*, federalsimi.it, 2020/6, p. 195; - Tizzano A., *Sui*

A conferma di ciò, si osservi che, da un lato, gli artt. 12 e 13 dir. 2000/31 regolano probabilmente il safe harbour in termini generali ed astratti, senza riferimenti alla lite specifica: in tal senso è pure la lett. e) dell'art. 13, che condiziona il safe harbour alla coerenziazione/aggiornamento dei dati di cache rispetto alla fonti originarie. Dall'altro, invece, l'art. 14 lo fa riferendosi alla condotta tenuta nello specifico caso sub iudice: è solo se l'hosting provider non sa della specifica illiceità lamentata o se, sapendolo, provvede a rimozione/disabilitazione, che può fruirne. Se questo è esatto, risalta ulteriormente l'incongruenza tra hosting provider e il cons. 42: quest'ultimo, infatti, si riferisce alle condotte in generale tenute dal provider, cioè al suo modello di business, non a quelle tenute in una determinata vicenda storico-processuale.

7. La pretesa <<passività>> e l'attuale modello di business delle piattaforme

Si potrebbe superare il dato letterale e riferirlo pure agli hosting provider, sulla base dell'argomento, per cui esprime un'esigenza generale, nel senso che vada riferita a chiunque voglia fruire di un safe harbour per il caso di commissione di illeciti da parte dei suoi utenti. In alternativa si potrebbe invece far governare la fattispecie dell'hosting provider solamente dall'art. 14 dir. 31/2000 (e art. 16 d. lgs. 70/2003): soddisfatto quanto ivi richiesto, null'altro gli è richiesto per godere dell'esenzione[93]. Come detto sopra, infatti, in detti articoli non ci sono regole o requisiti equivalenti a quelli del cons. 42[94].

rapporti tra giurisdizioni in Europa, in *Il dir. dell'Un. Eur.*, 2019/1, § I e § V). Si sarebbe potuta tentare un'interepretazione estensiva o analogica dei *considerando*, anche se non sono disposizioni normative ma illustrazioni inserite nel preambolo dell'atto legislativo.

[93] A dire il vero non sarebbe peregrina l'intepretazione, per cui tale raginamento andasse esteso agli altri due tipi di provider. Sarebbe più che lecito infatti opinare che il requisito dela passività del ruolo è solo tendenziale e corrispondente al *quod plerumque accidit*, dato che figura solo nei considerando e che, se veramente fosse requisito della fattispecie di fruizione del safe harbour, avrebe dovuto venir indicato pure nell'articolato.

[94] Punto colto bene dalle conclusioni 09.12.2010 dell'AG nel caso *L'Oreal c. eBay*, C-324/09, § 141-142 (ma non seguito dalla C.G. 23.03.2010 che ai §§ 113-114-119 nemmeon menziona la questione)- e dall'App. Milano 07.01.2015 Yahoo c. RTI, § 26-27, censurando il giudice di primo grado 09.09.2011 come anche qui segnalato sopra.

Se si ipotizza di applicare il cons. 42 all'hosting provider, serve un ragionamento più approfondito. Teoricamente il servizio di hosting potrebbe effettivamente limitarsi a dare ospitalità ai materiali caricati o, per i motori di ricerca, a soddisfare le ricerche producendo un elenco di risultati. In tale caso però dovrebbero sostenersi facendo pagare un corrispettivo. Invece la scelta è stata quella di offrirli in modo (apparentemente) gratuito al grande pubblico (per questo chiamati *siren servers*[95]) e di riservare invece la richiesta di compenso per servizi aggiuntivi a coloro cui vengono forniti (inserzionisti, per lo più imprese) o comunque a coloro a favore dei quali vengono utilizzati i dati personali di chi naviga o ricerca "gratuitamente": "Google.. sussidia gli utenti mettendo a disposizione un ampio portafoglio di servizi gratuiti (ricerca, email, …) e rivende la loro attenzione agli inserzionisti pubblicitari con un pagamento <<a risultato>> (pay-per-click)" [96] (potrebbero però esservi dei servizi aggiuntivi "premium" a

[95] Da Jaron Lanier, cit. da Posner E.-Weyl G., *Radical marktets. Uprooting capitalism and democracy for a just society*, Princeton University Press, 2018, p. 220. V. nota seguente.

[96] Così Saviozzi F.A., *Imprendtorialità*, Egea-Pixel, 2017, p. 77. Le piattaforme dunque non lo fanno gratuitamente, ma a fronte del rilascio di consenso al trattamento dei dati medesimi: in altre parole, chiedono un corrispettivo non monetario. La dir. UE 2019/770 del 20.05.2019 sulla disciplina delle forniture digitali tocca il punto, quando, dopo aver detto di applicarsi alle forniture a fronte di un prezzo, dichiara di applicarsi <<*altresì nel caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico*>> (art. 3 § 1 c. 2). E' stato fatto notare che manca l'esplicitazione della corrispettività e che dunque la norma si riferisce al caso delle due prestazioni –esecuzione del servizio digitale/cessione dei dati o meglio del diritto di uso degli stessi – collegate si, ma solo "casualmente" anzchè sinallagmaticamente (Camardi C., *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in Giust. civ., 3, 2019, 505-511). L'opinione lascia perplessi, sia per un dato testuale che per una considerazione generale. Circa il primo, la formulazione non è diversa da quella della prima parte del § 1, relativa al prezzo, nella quale pure manca l'esplicitazione del nesso di corrispettività (<<*si applica a qualsiasi contratto in cui l'operatore economico fornisce, o si impegna a fornire, contenuto digitale o un servizio digitale al consumatore e il consumatore corrisponde un prezzo o si impegna a corrispondere un prezzo*>>); anche la seconda parte del § 1 andrà interpretata allo stesso modo, per cui, se è riferita ad operazioni di scambio la prima, ugualmente sarà per la seconda (con la particolarità che la controprestazione è qui costituita dal diritto di usare i dati personali: lo si desume in modo piano dai cons. 24-25). Avrebbe poco senso, del resto, che il legislatore disciplinasse due atti tra loro

collegati (in che modo, poi?) solo "per caso"; né c'è bisogno di soffermarsi sul fatto che la presenza dell'autorizzazione all'uso dei propri dati nelle condizioni generali di contratto non è "casuale". Circa la considerazione generale, nel "capitalismo della sorveglianza" (v. testo di Zuboff) l'apparente gratuità è notoriamente finalizzata (ed anzi attivamente promossa) proprio ad acquisire dati personali da usare soprattutto nel microtargeting, vera fonte dei (lauti) guadagni: non è nemmeno gratuità interessata, è proprio corrispettività. La sinallagmaticità è rilevabile *ictu oculi* nei fatti ed è comunque ravvisata ormai da tutta la dottrina specialistica, tra cui: - Perlingieri C., *Profili civilistici dei* social networks, ESI, 2014, p. 88 ss.; Ricciuto V., *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in Riv. dir. civ., 2020/3, 642 ss, passim (ad es. 652-653); Schneider G., *<<Verificabilità>> del trattamento automatizzato dei dati personali e tutela del segreto commerciale nel quadro europeo*, in *Merc. concorr. regole*, 2019, 2, 368; - Resta G.-Zeno-Zencovich V., *Volontà e consenso nella fruizione dei servizi in rete*, RTDPC, 2018/2, 416; - J. Drexl, R. M. Hilty, L. Desaunettes, F. Greiner, D. Kim, H. Richter, G. Surblytė, K. Wiedemann, *Data Ownership and Access to Data. Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate*, ssrn.com, posted 06.09.2016, p. 3, § 7 (all'interno di un discorso volto ad escludere la necessità di un nuovo diritto esclusivo per i dati personali); - AGCM-AGCOM-Garante Privacy, *Indagine conoscitiva sui* Big Data, 10.02.2020, p. 89, ad es. in www.agcm.it); - Talia D., *La società calcolabile e i big data*, cit., 47-8; - Thobani S., *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *Riv. dir. media*, medialaws.eu, 2019/3, §§ 2-3, passim (per la quale giustamente è pratica commerciale scorretta affermare la gratuità del servizio - come un noto social faceva fin a qualche tempo addietro, facendo comparire la scritta "È GRATIS E LO SARÀ SEMPRE"); - OECD, *Quality considerations in digital zero-price markets. Background note by the Secretariat*, 28.11.2018, passim (spt. cap. 1, §§ 1-10), ove ampio esame (tra cui ad es. la questione della applicabilità della tutela consumeristica nelle *non monetary transactions*, cui viene data – comprensibilmente- risposta positiva: § 137); - Kolt N., *Return on data: personalizing consumer guidance in data exchanges*, *Yale law§ policy review*, vol. 38, 2019, 77 ss, passim (lavoro interessante: v. ad es. sub II.A, p. 83 ss e 107-110 sull'oscuramento del sinallagma operato dalle piattaforme col tenere distinti i *terms of service* dalla *privacy policy* e p. 121 ss sui casi espliciti di vendita di dati a piattaforme); - Newman J.M., *The Myth of Free*, *The George Washington Law Review*, vol. 86/2, marzo 2018, 513 ss, spt. 553-554 e poi 556-563 sulle ragioni storico-socio-economiche (anticipate in sintesi a p. 517) della nascita del fenomeno, indicato anche come *Zero-price Effect*. Sinallagmaticità ammessa pure da Google nelle cause statunitensi in tema di violazione della privacy (McKinnon K., *Nothing Personal, It's Just Business: How Google's Course of Business Operates at the Expense of Consumer Privacy*, 33 *J. Marshall J. Info. Tech. & Privacy L.* 187 (2018), passim, ad es. 193, 199, 204) e pure riconosciuta come parte del suo business da alcuni giudici (McKinnon K., *Nothing Personal*, cit., p. 201-202). Ritengono riduttivo limitarsi alla contrattualità del rapporto Fourcade M.-Kluttz D.N., *A Maussian bargain: accumulation by gift in the digital economcy*, in *Big data§ society*, January-June 2020, 5/6 che ravvisano un *<<Maussian bargain>>* e cioè una più ampia relazione per la fruizione della *digital gift offering* (cioè il servizio internet volta per volta in questione), servizio di cui l'utente di fatto non può fare a meno. La formulazione ampia della disposizione può essere allora spiegata o come scarsa precisione dogmatico-

concettuale o come intento di comprendere proprio questa (oggi pervasiva) modalità di business e dunque di evitare fastidiose eccezioni di inapplicabilità da parte dei fornitori digitali, basate su una formulazione del documento contrattuale che strategicamente nasconda la corrispettività e palesi una apparente gratuità (per non dire che, probabilmente, si dovrebbe applicare in via analogica anche negando la corrispettività e ravvisando la gratuità interessata). Nella proposta iniziale della Commissione, però, la sinallgmaticità della prestazione era espressa ed era detto che quest'ultima poteva assumere la forma del prezzo o della cessione dei dati personali (art. 3 § 1, Proposta di dir. COM/2015/0634 final - 2015/0287 (COD) del 09.12.2015 e Cons. 13). Resta incerto se se in tali casi il consenso dell'utente (non solo consumatore, direi) sia realmente prestato in modo libero, secondo il parametro posto dall'art. 7 § 4 reg. GDPR 2016/679 (per non dire del se si tratti di regola di validità o solo responsabilità: esclude la prima Caggia F., *Il consenso al trattamento dei dati eprsonali nel diritto europeo*, Riv. dir. comm., 2019, 4, 423): - Basunti C., *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contr. impresa*, 2020/2, § 4, 882 ss; - Mantovani A., *Questioni relative al trattamento dei dati personali per finalità di marketing e profilazione*, Working Paper Series No. 3/2019, medialaws.eu, (testo all'altezza della nota 66), in senso negativo; - ampio esame del meccanismo di consenso informato -*notice and consent*- e della sua attuale sostanziale inutilità in Bietti E., *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, January 1, 2020). 40 Pace L. Rev. 307 (2020), letto in ssrn.com (spt. parte III, per cui esso fa gli interessi delle piattaforme invece che dei consumatori: dando il consenso, costoro <<they are in fact agreeing to a number of hidden forms of intrusive and manipulative data collection, use and storage practices, interferences, and opaque treatments>>, p. 365, e parte IV, ove spiega come anche gli interessi collettivi siano messi a repentaglio da questa prassi commerciale, sia perché producono danni a terzi –ad es. autorizzando a vedere informazioni concernenti la rete di amici [ma si può obiettare che questi l'hanno a loro volta accettato] sia perché concerne diritti inalienabili o indisponibili), - negano che si tratti di vero consenso Kim N. S.-Telman D.A. J., *Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent* (March 3, 2015), 80 Missouri Law Review 723 (2015), 723 ss, parte I, 730-744: gli aa. riferiscono –p. 737 ss.- di rilevazioni statistiche secondo cui i consumatori non gradiscono il data mining e la pubblicità personalizzata ed inoltre non sanno che le Big Tech usano i dati non solo per migliorare l'offerta, ma ad es. vendendoli ad altre imprese, se non addirittura dandoli in esame allo Stato (il quale preferisce –comprensibilmente- procurarseli così, anziché raccoglierli in prima persona: v. l'interessante lavoro di Rozenshtein A.Z., *Surveillance Intermediaries*, 70 Stanford Law Review, 1, gennaio 2018, 112-113, per il quale ricorrono ragioni sia pro che contro –dal punto di vista delle Big Tech Companies- all'adesione a tali richieste governative, 115 ss); - lo nega pure il *Bundeskartellamt* nella ponderosa decisione antitrust contro Facebook del 06.02.2019, caso B6-22/16, leggibile pure in inglese nel sito dell'Autorità tedesca, sub II.3.c.(2) ai §§ 639-665 (ma in realtà andrebbe letto tutto il II.3.c *No justification under Article 6 and Article 9 GDPR* o almeno l'ineccepibile ragionamento condotto in II.3.c.(3).(a) rubricato *Article 6 (1b) GDPR does not apply when the contractual contents are imposed unilaterally by the dominant company*, §§ 668 ss), con revoca però 23.06.2020 da parte del BGH dell'inibitoria già concessa in via provvisoria dal giudice di appello, sicchè Facebook deve per ora conformarsi al decisum dell'Autorità (Witt AC., *How Germany Managed to Outlaw Facebook's Core Business Model*, promarket.org,

10.07.2020). La corrispettività è espressamente rilevata dal cons. 16 del codice europeo delle comunicazioni elettroniche (dir. UE 2018/1972 dell'11 dicembre 2018) ed affermata da TAR Lazio 10.01.2020, sez. I, n. 260 (e 261), *Facebook c. Altroconsumo+1*, § 6-Diritto (ma anche §§ 7-10), rigettando così l'eccezione – proposta da FB- di carenza di potere in capo ad AGCM, trattandosi semmai di violazione della privacy e non di pratica commerciale scorretta ex cod. cons. (l'AGCM più cautamente ravvisa <<*di fatto uno scambio implicito tra gli utenti e la piattaforma*>> nell'interessante *Osservatorio sulle piattaforme online*, dicembre 2019, § 3.2, ma si v. tutto il § 3 *Economia dei dati*). Si pone anche un problema di (eventuale) abuso di posizione dominante per chi è in grado di eseguire profilature come nessun altro competitor: si v. ad es. l'approndito studio del Garante della concorrenza britannico, *Online platforms and digital advertising-Market study interim report*, 18.12.2019 (spt. cap. 5, ove *Initial findings*, §§ 5.283-5.290) nonché, circa Facebook, il provvedimento contenente un accertamento in tal senso emesso il 6 febbraio 2019 dal Bundeskartellamt tedesco, secondo quanto riferiscono D'Acquisto G.-Pizzetti F., *Regolamentazione dell'economia dei dati e protezione dei dati personali,* in *Anal. giur. dell'econ*., 2019, 1, 95-97, ove l'abuso consisterebbe nella capacità di raccogliere e incrociare dati da più fonti –Facebook, Instagram, Whatsapp, terze parti, forse a seguito dell'uso da parte di queste della procedura di identiicaizone via FB -, cosa non possibile per altri (si potrebbe dubitare che questo fosse un abuso o invece solo la dominanza: ma da un lato bisognerebbe leggere il provvedimento tedesco e dall'altro la risposta non è semplice e qui fuori luogo) (è la decisione cit. sopra in questa nota): anche se l'impugnazione ha portato alla sospensione cautelare della decisione (Oberlandesgericht Düsseldorf 26 agosto 2019, VI-Kart 1/19 (V), come leggo in C. Osti, R. Pardolesi, *L'antitrust ai tempi di Facebook*, in *Merc. Concorr. Regole*, 2019, 2, 195 ss, § 5 sull'impugnazione). Il vantaggio, dato più dall'enorme massa di dati a disposizione, che dalla qualità degli algoritmi, caratterizzerebbe pure Google (Gray J.E., *Google Rules. The History and Future of Copyright Under the Influence of Google*, Ox. Un. Press, 2019, 135 ss; suggerimenti per ridurne l'enorme potere a p. 151 ss). Disciplina la *sale of the consumer's personal information* il recente *California Consumer Privacy Act of 2018* (in vigore dall'01.01.2020), che ha inserito il tit. 1.81.5 nel Civil Code (Division 4, Part 4), con ampia definizione però del concetto: <<.*"Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.*>> (§ 1798.140, lettera (t): ho riportato solo il primo comma di tale lettera): si tratta di legge importante, in quanto prima disciplina generale sulla *data protection* negli Stati Uniti (ma già ampie critiche, ad es. in Alpert D., *Beyond request-and-respond: why data accesa will be insufficient to tame big tech*, in *Columbia law review*, vol. 120/5, sub II, p. 1234 ss; studio comparativo in Park G., *The Changing Wind of Data Privacy Law: A Comparative Study of the European Union's General Data Protection Regulation and the 2018 California Consumer Privacy Act*, in 10 *U.C. Irvine L. Rev.* 1455 (2020). esaminando le differenze soprattutto circa l'opt in/opt out e il diritto all'oblio, sub II, p. 1473 ss). Ampio esame dei profili antitrust (tra i molti saggi reperibili) in Bamberger K.A.-Lobel O., *Platform market power*, in *Berkeley technology law journal*, vol. 32/3, 2018, 1051 ss.

pagamento[97], magari privi di inserzioni pubblicitarie[98]). E' noto però che, circa tutela della data protection, la natura del consenso espresso è discussa[99] (per non dire che taluno muove critiche radicali alla scelta del consenso come baluardo della privacy)[100]. E' stato osservato che questo modus operandi sia frutto di un mutamento del modello di business: inizialmente Google (che fece da battistrada, gli altri seguirono) intendeva offrire servizi a pagamento, ma senza pubblicità, e solo dopo scelse l'opposta soluzione[101].

[97] Palmieri A., *Profili giuridici delle piattaforme digitali*, cit., 24. O anche, talora, *fremium* (free+premium): Gerbaudo P., *I partiti digitali. L'organizzazione politica nell'era delle piattaforme*, Il Mulino, 2020, p. 94.

[98] Bamberger K. A.-Egelman S.-Han C.-Elazari A.-Reyes I., *Can You Pay For Privacy? Consumer Expectations and the Behavior of Free and Paid Apps*, in *Berkeley Technology Law Journal*, Vol. 35/1, 2020, 327 ss. (spt. sub II.A, p. 336 ss.) comparano tramite studi empirici le applicazioni a pagamento (e dunque *ad-free*) a quelle (parallele) senza esborso monetario, ma gravate da *advertisment* (in un modo o nell'altro deve esserci il ricavo per la piattaforma!): constatando (cosa non molto sorprendente, purtroppo) che le prime non sono poi così prive di tracciamento dati, nonostante l'aspettativa in tale senso rilevata presso gli utenti (risultati sub III, p. 347 ss). La grande divergenza tra aspettative e realtà induce gli autori a suggerire intervento regolatorio (p.354/9).

[99] Secondo un a. infatti, il consenso al trattamento è in realtà un'autorizzazione (di tipo integrativo) che, in caso di operazione contrattuale, si aggiunge al (quindi non coincide col) consenso contrattuale (Bravo F., *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il connseso dell'interessato tra autorizzazione e contratto*, in *Contr. e impr*., 2019/1, 34 ss, passim). L'articolata proposta ricostruttiva è fonte di spunti di riflessione, ma alla fine non persuade: che i poteri del titolare del trattamento siano conformati per legge e che l'interessato possa sempre recedere, significa solo che il contenuto del contratto è in parte predeterminato, anche tramite una facoltà di recesso ex lege. Per cui, da un lato, dire che il consenso integra poteri di cui il titolare già dispone (da qui la presunta struttura autorizzatoria), non pare esatto, non riuscendosi a vedere il titolo giuridico di tale disposizione (nei casi in cui il titolare non può prescindere dal consenso stesso, naturalmente: v. art. 6 §1 GDPR): anche perché l'interessato potrebbe cedere l'uso dei propri dati a più titolari per trattametni diversi, sicchè sarebbe arduo dire che ciascun di questi titolare già dispone del poter di trattare i dati solo che venga eliminato l'impedimento tramite autorizzazione. Dall'altro lato, la duplicazione degli atti di volontà non pare necessaria, trattandosi solo di un particolare programma contrattuale, su cui la legge restringe l'usuale libertà di determinazione del contenuto: per cui, applicando il noto rasoio (*entia non sunt multiplicanda sine necessitate*), la dichiarazione di consenso può benissimo rimanere una sola.

[100] Cohen J. E., *Turning Privacy Inside Out*, forthcoming in *Theoretical Inquiries*, 2019, p. 6-11 (letto in ssrn.com).

[101] Posner E.-Weyl G., *Radical marktets*, cit., pp.209-213. Dato lo scambio servizi internet contro dati personali, non è chiaro perchè un a. abbia scritto che

Se si tiene conto di ciò, è ovvio che il provider spingerà al massimo per la fruizione dei contenuti caricati dagli utenti: da un lato, è proprio così che vengono raccolti i dati (le tracce) lasciate dai navigatori ì/fruitori[102] e, dall'altro la maggior

questi ultimi siano "*un capitale liberamente attinto senza neppure oneri compensativi dalle grandi aziende del digitale*" (Soro A., *Democrazia e potere dei dati. Libertà, algoritmi, umanesimo digitale*, Baldini+Castoldi, 2019, 29): la "compensazione" (rectius: controprestazione) dell'acquisto del diritto sui dati è costituita proprio dai servizi internet offerti (posta elettronica, motore di ricerca, social network, predisposiizone del marketplace etc.). E' noto che molti degli spazi pubblicitari sono allocati agli inserzionisti tramite aste in tempo reale, c.d *real-time bidding* (tramite ad es. la piattaforma *Doubleclick* per Google: v. Casilli A.A., *Schiavi del clic*, cit., p. 60): si v. (soprattutto sugli aspetti della scarsa competitività e della opacità all'inserzionista) l'eccellente indagine dell'Autorità inglese per la concorrenza CMA-Competition and Markets Authority, *Online platforms and digital advertising. Market study. Final report*, 1 luglio 2020, cit. pure infra, passim, ma soprattutto i *Findings* §§ 16-68 dell'*Introduction* (pp. 9-21) e i §§ 5.5-5.36, (pp. 213-222). Ci sono sospetti (manco a dirlo!) di pratiche collusive in queste aste per le inserzioni pubblicitarie su internet: v. lo studio in termini economico-matematici di Decarolis F.-Goldmanis M.-Penta A., *Marketing Agencies and Collusive Bidding in Online Ad Auctions*, 2017-2019, NBER Working Paper No. 23962, The National Bureau of Economic Reasearch.

[102] E' proprio fruendo dei contenuti disponibili sulle piattaforme, che i navigatori ricevono la pubblicità, per cui più contenuti vedono, qualunque essi siano, più pubblicità ricevono; dal lato opposto, una piattaforma, quanto più è diffusa e utilizzata, maggiore è il prezzo che può chiedere ai venditori per le inserzioni pubblicitarie. Nulla di nuovo, in fondo. Che alle piattaforme interessi solo il tempo di permanenza in esse (c.d. *engagement*), e nulla dei contenuti così fruiti, costituisce dato comunemente accettato: *<<the more searches, the better the predictions, and the better the predictions, the more the search engine is used>>* (Iansiti M.-Lakhani K.R., *Competing in the Age of AI. How machine intelligence changes the rules of business*, in *Harvard business review*, January Febrary 2020, 63). V. ad es.:- Da Empoli G., *Gli ingegneri del caos*, cit., 49, secondo cui "*l'intera architettura di Facebook§Co è basata sul nostro bisogno di essere presi in considerazione (…) [e] <<sfrutta un punto debole della psicologia umana. Gli inventori … ne erano perfettamente coscienti. E l'abbiamo fatto comunque >>... La macchina onnipotente dei social network, fondata sugli impulsi più primordiali della psicologia umana,non è stata concepita per darci tranquillità. Al contrario, è stata pensata per tenerci in una condizione di incertezza e frustrazione permanente*" (p. 65/66; nella parentesi quadra è riportato il pensiero di Sean Parker, cofondatore di Napster e uno dei primissimi collaboratori di Facebook); - Cohen J.E., *Law for the platform economy*, *Univ. of California Davis law review*, 2017, vol. 51, sub I.D e sub II.C, p. 145 ss e risp. p. 161 ss. Al punto da prevedere che le pubblicità (in base all'elaborazione di *like*, condivisioni e simili) giungano proprio nel momento in cui gli utenti pongono minor resistenza (ad es. quando gli adolescenti si sentono *worthless* e *insecure*: Susser D.-Roessler B.-Nissenbaum H., *Online Manipulation: Hidden Influences in a Digital World* (January 2020), 4 *Georgetown Law Technology Review*, 2019, 1 ss., passim (spt. II.A e V.B.2), i quali spiegano perché la comunicazione online

permanenza in rete aumenta gli spazi pubblicitari[103]. I likes (ora

è particolarmente adatta alla manipolazione in Id., *Technology, autonomy, and manuipulation*,, *Internet policy review*, vol. 8/2, 2019, 6-7 ma anche 9-11); Domer P., *De Facto State: Social Media Networks and the First Amendment*, Notre Dame L. Rev. 893 (2020), 916; Reilly M., *Is Facebook targeting ads at sad teens?*, MIT Techlogy Review, 1 maggio 2017 ; un po' generico Lavi M., *Evil Nudges*, *Vanderbilt Journal of Entertainment & Technology Law*, 2018, vol. 21, 15, quando osserva: <<*Some business models are based on nudges that enhance extreme or offensive content to attract users and, in turn, increase advertising revenue*>>. Gli studiosi del marketing, allora, preso atto che, soprattutto a causa dell'evoluzione dei telefoni portatili in computer, il collegamento alla rete è costante, affermano la necessità di un diaologo pure costante dell'azienda con i consumatori, a fini di una profittabilità durevole (questa è l'idea base di tutto il libro di Mandelli A.-Arbore A., *Marketing digitale*, Egea-Pixel, 2 ed., 2019, ad es. 13/14, 20/1, 56/8, ove le espressioni *continuous learning* e di *social ubiquitous management*, 71, 90-93, 103-104, 133, 144/ ove si scrive di <<spostamento di attenzione dalla transazione alla relazione con i clienti>>). Anche quando non interagiscono con gli utenti, c'è l'interesse a raccogliere dati non personali di vario tipo tramite i software di *web scraping*, i quali scandagliano -tramite i c.d bot- i siti internet di interesse: ad es. per per monitorare in automatico i prezzi dei concorrenti, implementare il mercato dei *big data analytics* o raccogliere dati per allenare i sistemi di AI fondati sul *machine learning* (così Monterossi M.W., *Estrazione e (ri)utilizzo di informazioni digitali all'itnerno della rete internet. Il fenomeno del c.d.* web scraping, in *Dir. informazione informatica*, 2020/2, 331-332; l'a esamina le possibili tutele tramite: -disciplina delle banche dati, p. 336 ss-; regime contrattuale con i <*termini d'uso*> dei siti web, p. 346 ss.; - misure tecnologiche di protezione, p. 357 ss.; tutela concorrenziale, p. 362 ss).

[103] La ricerca incessante di "approvviginamento" di (dati degli) utenti è ricordata spesso nell'importante libro di Zuboff S., *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss ed., 2019 (ad es. §§ 5.2-5.3, pp. 141-166: "ogni risposta umana a ogni suggerimento comermciale offre più dati che possono portare a prodotti predittivi più efficaci … C'è molto in gioco in questa frontiera del mercato, nella quale *un comportamento imprevedibile equivale ad un guadagno perso*", p. 165, corsivo nel testo; l'a. scrive di "testo ombra" (oltre al "primo testo", di cui l'utente è consapebole) per rifersi alla profilazione, di cui l'utente è invece inconsapebole, pp. 199 e 217, tramite la c.d. renderizzazione e cioè la tecnica per trasformare appunto le esperienze on line in dati, p. 247-249). Anche il problema delle fake news è ambiguamente affrontato dalle Big Tech: anzi You Tube ne trae buon profitto (così l'interessante lavoro di Manheim K.-Kaplan L., *Artificial Intelligence: Risks to Privacy and Democracy*, *Yale Journal of Law & Technology*, 2019, vol. 21, 106 ss, a 147/8). Stante la cennata struttura del capitalismo della sorveglianza, dunque, non sono pertinenti i richiami al libro *1984* di George Orwell, dato che oggi, a differenza della situazione ivi immaginata, sono gli stessi *cives* a darsi attivamente da fare per essere sorvegliati: così Lyon D., *La cultura della sorveglianza. Come la società del cotnrollo di ha reso tutti controllori*, LUISS University Press, 2020 (orig.: 2018), ad es. p. 18 ss. e p. 124 ss. -ma il tema costituisce uno dei *Leitmotive* del libro-; e l'a. chiosa, data la pervasività del controllo, che <<*oggi l'assunto, che se non hai niente da nascondere, non hai niente da temere, è sistematicametne minato dalla nuova*

gli emojis) di Facebook, ad es., solo apparentemente sono un modo per esprimere giudizi o sentimenti verso altre persone: in realtà sono stati creati per tracciare in modo sempre più preciso l'utente, senza il fastidio e l'impegno che avrebbe creato l'analisi di centinaia di post di commento[104]. Facebook lo dice apertamente, ad es. nei documenti allegati al bilancio, con dichiarazione che vale la pena di riportare: <<*The size of our user base and our users' level of engagement are critical to our success. Our financial performance has been and will continue to be significantly determined by our success in adding, retaining, and engaging active users of our products, particularly for Facebook and Instagram. We anticipate that our active user growth rate will continue to decline over time as the size of our active user base increases, and it is possible that the size of our active user base may fluctuate or decline in one or more markets, particularly in markets where we have achieved higher penetration rates....If we are unable to maintain or increase our userbase and user engagement, our revenue and financial results may be adversely affected. Any decrease in user retention, growth, or engagement could render our products less attractive to users, marketers, and developers, which is likely to have a material and adverse impact on our revenue, business, financial condition, and results of operations. If our active user growth rate continues to slow, we will become increasingly dependent on our ability to maintain or increase levels of user*

sorveglianza>> (p. 91-92), anche dovuta al passaggio dall'*online* all'*onlife*, secondo la brillante espressione di Luciano Floridi, e cioè all'always on, connessione ininterrotta (ivi p. 121 ss). In sintesi, <<*la cultura della sorveglianza.. diventa la nuova normalità. La sorveglianza non è più la circostanza eccezionale, l'ultima spiaggia, l'indagine specifica che si pensava fosse nelle società liberal-democratiche, che si affidano al controllo giuridico per protgeggere i cittadini dagli eccessi*>> (Lyon D., *La cultura della* sorveglianza, cit., p.129).

[104] Così Casey B.-Lemley M.A., *You might be a robot*, in *Cornell law review*, 2020, 322-323, per i quali l'iniziale introduzione dei pulsanti *like* fu un atto di *aesthetic genius* (il saggio passa poi ad affrontare il problema di individuare ciò che costituisce *robot* a fini normativi, suggerendo un approccio non definitorio ma funzionale: v. spt. sub III.A-B, p. 341 ss). Non solo i like costituiscono un fattore produttivo per il continuo miglioramento del servizio offerto dalla piattaforma, ma molte altre condotte tenute on line dall'utente (commenti, critiche, resoconti, voti, stelline etc.): v. Casilli A.A., *Schiavi del clic*, cit., p. 79-80 e p. 137 ss sui *prod*user (*producer+user*; ma si v. l'intero cap. 2, p. 59 ss., *Di cosa parliamo quando parliamo di piattaforma digitale*).

engagement and monetization in order to drive revenue growth>>[105]. Impostazione che soddisfa (o dovrebbe soddisfare) sia l'utente, proponendo contenuti "gratuiti" analoghi a quelli già visti e dunque presumibilmente graditi, sia i venditori, indirizzando le loro proposte di vendita verso i navigatori che - dai dati ubiquamente raccolti- risultano più probabilmente interessati[106]. Si chiama *stickiness*, cioè appiccicosità: la

[105] Trautman L.J., *Governance of the Facebook Privacy Crisis*, *Pittsburg Journal of Technology Law & Policy*, vol. 20/1, 2020, pp. 69/70, ove anche ampio esame del modello di business di Facebook (spt. sub II *The Business of Facebook* e sub V *Risk Factors*).

[106] E' stato osservato che mentre in un primo momento la tracciatura era utilizzata per individualizzare e quindi migliorare le proposte ai navigatgori (quindi ottica rivolta a costoro), in un secondo momento i big player del settore (in primis google) hanno scoperto l'enorme valenza commerciale e dunque redditività dell'applicazione dei dati alle esigenze non più dei navigatori ma delle imprese inserzioniste (quindi ottica rivolta a costoro). Il passaggio (nitidamente individuable) è descritto dall'importante libro Zuboff S., *Il capitalismo della sorveglianza*, cit.. Un recensore italiano ritiene non convincente il collegamento diretto dell'a. tra mniapolazione dei dati e dinamiche capitaliste (C. Bastasin, *Siamo tutti sorvegliati speciali*, Il Sole 24 ore, 27.10.2019, p. 30). Sono già uscite diverse attente recensioni del libro di Zuboff: ad es. Cuellar M.F.-Huq A.Z., *Economies of surveillance*, *Harvard Law Review*, febbraio 2020, vol. 133, n. 4, 1280 ss. Gli aa. muovono diverse critiche: v. spt. la critica al'assunto di base per cui il *surveillance capitalism* acquisirebbe illecitamente infomazioni private, e comprometterebbe l'esericzio del libero volere e l'interiorità psicologica necessaria per una personalità sana (p.1314 ss, sub B-C-D) e all'asserita radicale discontinuità rispetto al capitalismo rpecedente (p.1298 ss., p.1320 e p.1326); v. pure la positiva valutazione di alcuni aspetti del *surveillance capitalism* che invece parrebbe irrimediabilmente condannato da Zuboff (p. 1311 ss). Tra le critiche v. anche quella della inesattezza del termine "capitalismo della sorveglianza" che, facendo pensare ad un unico tipo di business (quello di Google e Facebook), non tiene conto della pluralità invece di altri tipi che pur si appoggiano al *data mining* e in particolare dei diversi modi di massimizzare il *behavioral surplus* (finanza, assicurazioni, sanità, immobiliare: ivi, sub II.C, p.1298, p.1304-1309, p.1325; per questo propongono "Economie della Sorvegliazna/*Surveillance Economies*"). Tuttavia, impregiudicata la questione della esistenza e dimensione di tali diversità, il termine "capitalismo della sorveglianza" non fa affatto riferimento ad un solo modo di rapportarsi al data mining: indica invece la generale caratteristica per cui oggi quasi tutte le attività economiche (di certo tutte le maggiori in termini dimnensionali e di diffusione) hanno bisogno di sempre più dati per rimanere sul mercato e ciò comporta una conoscenza analitica ed estesa delle persone, che alla fine può dirsi sorveglianza. Del resto la vorace necessità di dati per tutti i maggiori player di tutti i settori viene soddisfatta in pratica solo dalle Big Tech, che paiono dunque in pratica diventate i reali gatekeepers della comnuncazione commerciale e non. Tanto che ora il settore tecnologico è inserito tra quelli (oltre al finanziario) che costituiscono fonte di rischi sistemici (Welburn J.W.- Strong a. ed altri, *Systemic Risk in the Broad Economy. Interfirm Networks and Shocks in the U.S.*

Economy, a cura della Rand Corporation, 2020). Oppure v. la recensione di Kapczynski A., *The law of informational capitalism*, *The Yale Law Journal*, 2020, vo. 129, 1460 ss, che, pur apprezzando l'esame dei mecanismi di sorveglianza (1467 ss.), rimprovera a Zuboff di essersi concentrata solo sulla libertà individuale, dimenticando: 1) le gravi conseguenze collettive e cioè i profili antitrust, stante l'enorme potere di cui le piattaforme dispongono, oggi che la presenza ivi è necessaria per qualunque operatore (p.1473 ss; p.1489 per gli effetti di rete: per una descrizione dei vari vantaggi che la dimensione offre alle Big Tech v. Hindman M., *La trappola di internet. Come l'economia digitale costruisce monopoli e mina la democrazia*, Einaudi, 2019 (orig.: 2018), cap. 2, *Un gioco sbilanciato* p. 20 ss) ; 2) che questo capitalismo non è si è sviluppato al di fuori dell'ordinamento giuridico (*lawlessness*), come vorrebbe Zuboff, ma, all'opposto, sfruttandone tutte le opportunità (proprietà intellettuaole, p.1499; riserve contrattualmente pattuite e tutela dei segreti commerciali, p.1501 ss), tema invece centrale nell'altro libro ivi recensito (Cohen J. E., *Between truth and* power, cit., cap. I per gli strumenti giuridici usati dalle Big Tech: contratti e tutela dei segreti); per precisare in conclusione che il diritto è usato da questi colossi aziendali non solo per ottenere e consolidare il potere, ma anche per sottrarlo al controllo democratico, soprattutto in tre modi: i) le taking clauses (indennizzi da esproprio quando lo Stato vuol conoscere l'algoritmo); ii) il riconoscimento alle Big Tech del diritto di espressione: e qui v. la tesi (French W., *This Isn't Lochner, It's the First Amendment: Reorienting the Right to Contract and Commercial Speech*, in *Northwestern University Law Review*, 2019, vol. 114/2, 469 ss) per cui, pur distinguendo tra discorso solo comunicativo e le condotte conseguenti (ivi, p. 491) e quindi non attribuendo in toto alle imprese la libertà di parola, comunque risconosce l'ombrello protettivo del Primo Emendamento almeno al tentativo di persuadere altri a tenere certe condotte (ad acquistare) e cioè in breve lo riconosce alla pubblicità commerciale (ivi, 495-496); iii) la creazione di organismi su misura come il WTO (p.1508 ss). Decisamente critica l'approfondita recensione di Morozov E., *Capitalism's new clothes*, 04.02.2019, *thebaffler.com*, per il quale, visto che il vero pericolo temuto e denunciato da Zuboff è la modifca dei comportamenti tramite la sorveglianza, sarebbe stato pù esatto chiamarlo ad es. "*behavior modification capitalism*" invece che "*surveillance capitalism*" (§ XII; l'esame vero e proprio del libro è ai §§ IX segg.; nella prima parte il recensore ricorda il percorso intellettuale di Zuboff e il suo legame con l'impostazione teorica dello storico dell'economia Alfred Chandler, soprattutto circa il concetto di *managerial capitalism*¸§§ II-V, che Z. propone oggi di sostituire con quel tipo di *distributed capitalism*, che è l'*advocacy capitalism* tipo quello praticato da Apple, fine § V-inizio § VI). Sostanzialmente positiva invece la recensione di Wu T., *Bigger brother*, in *The New York Review of Books*, 9 aprile 2020, il quale, dato lo strapotere di controllo dei flussi dei dati, conclude così: "*That's why we must dare to say what would sound like blasfemy in another age. It may be that a little less knowledge is what will keep us free*". Recensione italiana (assieme a quella di altri due testi) in Sartori L., *Sorvegliati dal web*, in *Il Mulino*, 2020/4, p.711 ss. Attribuisce all'algoritmo di Facebook, che gestisce la pubblicità (advertising algorithms) collegandola al *newsfeed*, la natura di *speech* (anzi, di *commercial speech*), coperto dal Primo Emendamento, Thompson K.A., *Commercial Clicks: Advertising Algorithms as Commercial Speech*, in *Vanderbilt Journal of Entertainment & Technology Law*, 2019, vol.21/4, 1019 ss, spt. III.A.1-2, 1031-1036 (ammettendone però una certa regolamentazione, come sollecitato dallo stesso Zuckerberg): lascia però perplessi il fatto che l'a. non distingua nettamente

capacità delle aziende di attrarre gli utenti, di farli rimanere il più a lungo possibile e di farli tornare più e più volte[107]; cosa che tra l'altro ha indotto un a. a ravvisare un regresso verso posizioni passive (push invece che pull, lean back invece che lean forward, passive invece che active) dell'audience rispetto ai mezzi di comunicazione antecedenti e soprattutto rispetto alla televisione[108]. E' stato significativamente osservato che <<*accumulare un pubblico on-line e come pompare aria in un pallone con una lieve perdita. Bisogna continuare a pompare*

tra l'algoritmo, che regola la diffusione dei post degli utenti –newsfeed-, e quello che regola l'advertisement connesso, dato che il trattamento giuridico deve essere diverso. Il riconoscimento della copertura del Primo emendamento agli enti commerciali è tema importante e assai esaminato, qui non affrontabile: mi limito a ricordare Cohen I. E., *Between truth and power*, cit., 94, per cui non esso discende necessariamente dalla Costituzione USA o dalla storia, ma è frutto di una lunga e attentamente progettata campagna legale e di publiche relazioni. Altro saggio, breve ma denso, sui profili generali questo tipo di impresa *data driven* è quello di Myers West S., *Data capitalism: redefining the logics od surveillance and privacy*, in *Business&society*, vol. 58/1, 2019, che con *data capitalism* intende descrivere le conseguenze <<*of the turn from an e-commerce model premised on the sale of goods online to an advertising model premised on the sale of audiences—or, more accurately, on the sale of individual behavioral profiles tied to user data. The term purpose-fully hearkens back to an earlier moment in media history, when the penny press supplanted partisan newspapers by focusing on the sale of advertising and commoditization of mass audiences. The advent of print capitalism in the 19th century marked a similar turn in media business models, from the sale of products—newspapers—to the sale of news corporations' audiences to subsidize media production. The value of advertising space and increase in street sales of cheap newspapers motivated press owners' pursuit of wide circulation to justify news revenues*>>, p. 23-24 (ove interessanti rierimenti storici sull'uso sempre più intenso dei dati dei potenziali clienti). Sul ruolo dei big data nell'economia attuale v. il report di IT Media Consulting, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, Roma, gennaio 2018 (col contributo scientifico di Univ. Bocconi), cap. II *L'economia dei dati*, p. 93 ss.

[107] Così Hindman M., *La trappola di internet*, cit., 4. Libro molto interessante, che analizza (in modo accessibile) sotto il profilo economico-gestionale l'attività delle piattaforme: ad es. v. il cap. 2, p. 20 ss., ove l'a. spiega perché sono economie di scala. Anzi quest'ultima considerazione è alla base di tutto il libro: v. capp. 4 e 5 ma anche dopo, ad es. p. 157 (impatto sull'informazione locale, 165 (il data mining chiede molti dati). 181 etc. (più aggiornamenti e conteuti nei siti=più traffico), 201 ss (sorta di sintesi). In altre parole, <<*the more time users spend on the platform, the more appealing that platform becomes to advertisers, who are then willing to spend more money to capture the attention of these users*>> (Grafanaki S., *Platforms, the First Amendment and Online Speech: Regulating the Filters*, cit., 125). Accenna a questo aspetto Giannone Codiglione G., *Internet e tutele di diritto civile*, cit., 163/4.

[108] Napoli P., *Social media and the public interest*, cit., 43 ss e 48 ss

per mantenere un livello costante di investimento, altrimenti il lavoro precedente si perde rapidamente. questi costi indiretti di distribuzione non sono opzionali per un sito di informazione o un blog mantenere un livello di stickiness *superiore alla media è una questione di vita o di morte*>>[109]. Ciò permette la c.d. profilazione, la quale è "una tecnica di trattamento (parzialmente) automatizzato di dati personali e/o non personali, finalizzata alla creazione di conoscenza predittiva mediante la scoperta di correlazioni tra i dati e la costruzione di profili, che possono essere poi utilizzati per assumere decisioni. Un profilo è un insieme di dati correlati che rappresentano un soggetto (individuale o collettivo). La costruzione di profili è il processo di scoperta di schemi ricorrenti e sconosciuti tra i dati, all'interno di grandi insiemi di dati, che possono essere utilizzati per creare profili. L'applicazione di profili consiste nell'identificazione e rappresentazione di uno specifico individuo o gruppo come corrispondente a un determinato profilo, e nel processo decisionale basato su tale identificazione e rappresentazione"[110]. I dati sono raccolti in qualunque modo, sia in proprio sia acquisendoli da terzi[111], al punto che tale massiccia e continua attività -quale corrispettivo non monetario della fruizione di servizi internet- è stata qualificata come <<*tecnofeudalism*>>[112],

[109] Hindman M., *La trappola di internet*, cit., 17. Vi accenna Quintarelli S., *Capitalismo immateriale*, cit., 89-90 e 188.

[110] Definizione di Bosco F.-Creemers N.-Ferraris V.-Guagnin D.-Koops B.J., *Profiling technologies and fundamental rights and values: regulatory challenges and perspectives from European Data Protection Authorities*, in *Reforming European data protection law*, Dordrecht, 2015, p. 8, non visto, cit. da Lagioia G.-Sartor G., *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in *Federalismi*, 2020/11, 24.04.2020, leggibile in *federalismi.it*, 91-92. Rilevata pure dalla sociologia dei consumi: Boltanski L.-Esquerre A., *Arrichimento. Una critica della merce*, Il Mulino, 2019 (orig.: 2017), 243-244. Un settore del *data mining* è quello della *sentiment analisys*, che cerca di catturare opinioni, preferenze e sensazioni delle persone sui più svariati temi (Talia D., *La società calcolabile e i big data*, cit., 101-102)

[111] Pasquale F., *The black box society: The secret algorithms that control money and information*, Harvard University Press, 2015, p. 30-34.

[112] Posner E.-Weyl G., *Radical marktets*, p. 230 ss; li segue Geddes K., *Meet Your New Overlords: How Digital Platforms Develop and Sustain Technofeudalism*, in *The Columbia Journal of Law & The Arts*, 2020, *43*(4), p. 478. L'induzione al deposito (e al trasferimento) dei dati nei servizi on line, pubblicizzando sottilmente il lato piacevole di questi ultimi, è paragonato al famoso stratagemma psicologico (economia comportamentale *in nuce*!) di Tom Sawyer per evitare di pitturare la staccionata e farlo fare agli amici, descrivendone

perché ricorderebbe il rapporto medievale tra il ricco possidente e il coltivatore (*serfs*, per vero scrive l'a.): rapporto in cui il secondo, a fronte del diritto di usare il fondo del primo, di trarne i frutti e di ottenere una qualche protezione, si obbligava[113] a trasferirgliene una parte[114]. Altri scrive invece a questo proposito di *data colonialism*, facendo un parallelo con lo sfruttamento colonialistico delle ricorse di paesi extraeuropei[115]. Naturalmente l'online behavioural advertising genera non piccoli problemi legati alla privacy e alla discriminazione[116], come ricorderò più avanti.

La profilazione, però, non è da esecrata da tutti, dato che altri

il grande piacere ritraibile (Posner E.-Weyl G., *Radical marktets*, p.233 ss. che dunque sostituiscono il *fence whitewashing* scon il *digital whitewashing*).

[113] Con quanta reale libertà di scelta è da verificare, ora (poca) come allora (probabilmente nulla). Gli aa. scrivono di *serfs*, per vero, non di coltivatori. I contratti agrari di associazione hanno in effetti una lunga storia e l'esempio più noto ed attuale da noi è il rapporto di mezzadria (art. 2141 cc) ove la divisione è fatta a metà.

[114] E' curioso che le modifiche radicali ai rapporti sociali introdotte dalla Rivoluzione Francese non abbiano però riguardato (ed abbiano dunque conservato) questo tipo di rapporti, in quanto a base contrattuale: v. Piketty T., *Capitale e ideologia*, La nave di Teseo, 2020 (or.: 2019), pp. 126-131.

[115] Couldry N.-Mejias U.A., *The costs of connection: how data is colonizing human life and appropriating it for capitalism*, Stanford University Press, 2019, parte I e II, non visto, ma recensito da Pettis B., *The costs of connection: how data is colonizing human life and appropriating it for capitalism*, in *Critical Studies in Media Communication*, 2020, 1 ss. Scrive del rischio di *digital colonialism* Bell E., *The unintentional press*, cit., 250 (circa Facebook).

[116] Questi i principali rischi esaminati da Wachter S., *Affinity Profiling and Discrimination by Association in Online Behavioural Advertising* (May 15, 2019), in *Berkeley Technology Law Journal*, Vol. 35, No. 2, 2020, forthcoming, letto in ssrn.com. L'a. approfondisce soprattutto l'*affinity profiling* e cioè la profilazione basata sulla rilevazione dei dati sensibili non diretta ma indiretta e cioè desunta dall'<<affinità>> (di vario tipo, come stabilita dall'algoritmo) con persone titolari dei dati sensibili: sostiene che pure questa profilazione per inferenza rientra nella data protection offerta dal GDPR e spt. dal suo art. 9 << Trattamento di categorie particolari di dati personali>> (p. 18 ss), come pure la discriminazione per inferenza rientra nell'ambito applicativo della *EU non discrimination law* (p. 22 ss e 31 ss.), anche quando avviene tramite la creazione di gruppi di persone tramite *inferential analytics* (p. 54 ss). Più sinteticamente e in versione giornalistica v. il report sugli studi di Wachter sul Financial Times del 12.12.2019, ediz. online, Murgia M., *Algorithms drive online discrimination, academic warns* (con paywall). V. poi ad es. (in una letteratura enorme) Pike E., *Defending Data: Toward Ethical Protections and Comprehensive Data Governance*, in *Emory law journal*, vol. 69/4, 2020, 693-696 sulla pervasività della raccolta di dati e p. 699 ss sui relativi rischi.

la ritiene anzi soddisfacente, in quanto meglio soddisfacente i bisogni personali: il vero problema starebbe invece nella cessione alle piattaforme del surplus di valore, di cui sono portatori i dati personali raccolti presso gli utenti, visto che sono le prime a trarne enormi guadagni, senza alcun ritorno per i secondi[117].

[117] Paglieri F., *La disinformazione felice*, cit., p. 226-229. Il discorso però qui non scorre bene: i) scrivere che non esiste problema di privacy, dato che chi fruisce di questi servizi internet non vi è interessato, può essere vero per alcuni ma non necessariamente per altri; ii) scrivere di "regalo" dei dati è errato, dato che costituiscono la controprestazione per la fruizione dei servizi internet (cosa che poi l'a. ammette, per cui forse è solo una svista); iii) scrivere che i dati ceduti <<hanno un valore ben maggiore della contropartita che ci è stata offerta>> è un po' frettoloso, anche se apre una questione interessante (cita infatti degli studi che tentano di determinare il valore dei dati forniti): tuttavia la risposta richiederebbe un esame approfondito e tutt'altro che facile. L'enorme guadagno delle piattaforme, infatti, è prodotto non solo dai dati raccolti, ma anche dalla loro archiviazione, catalogazione e reimpiego nella costruzione e vendita di spazi pubblicitari: il che richiede enormi capacità organizzative e dotazioni informatiche, che vengono predisposte dalle piattaforme e non dagli utenti: non a caso molti parlano di *big data* come *the new oil* (lo nega -in termini strettamente giuridici- Scholz L.H., *Big Data is Not Big Oil: The Role of Analogy in the Law of New Technologies* (September 20, 2018), in *Tennessee Law Review*, Forthcoming, letto in ssrn.com: ma, come che sia, non viene meno in termini economici il loro ruolo di uno tra gli altri fattori produttivi). In altre parole i dati hanno reale valore solo quando sono utilizzabili (in forma aggregata) da imprese opportunamente attrezzate: non ne hanno (o ne hanno molto meno), fino a che restano nella esclusiva disponiblità del titolare originario (così giustamente Kolt N., *Return on data*, cit., 91, precisando che ciò non ne fa venir meno la natura di corrispettivo). Ne segue che l'affermazione, secondo cui a costoro spetta una misura assai maggiore dell'utile prodotto da tale <concertazione di fattori produttivi> (c.d. *data dividend*), appare un po' semplicistica (forse si tratta di un auspicio; l'a. però non è un giurista e il libro, come detto, è di assai piacevole lettura). Senza dubbio è l'attività a giustificare il conseguimento del profitto, come ribadisce recente dottrina (Scozzafava O.t., *Delle risorse, dell'attività, del profitto*, in *Persona e mercato*, 2020/3, 199 ss, spt. §§ 5 e 9), anche se l'idea appartiene più al discorso economico che giuridico: secondo quest'ultimo, che si basa su schemi formali, il profitto spetta a chi si presenta come venditore e incassa il prezzo o corrispettivo, dopo detratti i costi relativi ai fattori produttivi in base ai rispettivi titoli giuridici. Il tema allora può costituire un ottimo banco applicativo del richiamato concetto di <concertazione di fattori produttivi>, venuto alla ribalta (dopo il pioneristico lavoro di Sacco R., *L'arricchimento ottenuto mediante fatto ingiusto*, Utet, 1959) con il trasferimento dei profitti ex art. 125 c.3 cod. propr. ind., soprattutto nel caso di violazione da parte di *multicomponent products* (problema del c.d *apportionment*, ma se ne discute anche per il risarcimento del danno: Reinecke J., *Lost Profits Damages for Multicomponent Products. Clarifying the Debate*, in *Stanford law review*, vol. 71, giugno 2019, 1621 ss, discutendo il caso *Mentor Graphics Corp. v. EVE-USA, Inc*. del 2017; Chao B.-O'Dorisio R., *Saliency, anchors & frames: a multicomponent damages*

Se si tiene conto di tale contesto socioeconomico[118], la

experiment, in *Michigan Technology Law Review*, vol. 26/1, 2019, sub I, p. 5 ss. e sub II, p. 9 ss sui due errori cognitivi *saliency bias* e *anchoring*): solo che in tale saggio si studia il caso di uso illecito di risorse altrui, mentre nel caso della profilazione quello di uso acconsentito. Si pone un problema analogo a quello sub iii) il lavoro di Kolt N., *Return on data*, cit. in questa nota, laddove stima eccessiva l'attenzione alla privacy, suggerendo invece un maggior controllo sul *return on data-ROD* (parafrasando il *return on investment-ROI* aziendale) e cioè sull'utilità che l'utente riceve in cambio: ROD rilevabile tramite apposite (future) applicaizoni, basate sulle metriche raccolte dalle Big Tech (Kolt N., *Return on data*, cit., sub V.A, p. 123 ss). Sul punto dell'estrazione del c.d. surplus comportamentale v. Zuboff S., *Il capitalismo della sorveglianza*, cit., passim ad es. pp. 85-92.

[118] Chiamato delle "piattaforme bilaterali" (in altri casi, *multisided platforms/ markets*, come ad es. quella trilaterale di Youtube: inserzionisti, utenti navigatori/spettatori e utenti uploader c.d youtuber, come osserva Casilli A.A., *Schiavi del clic*, cit., p. 60): si v. ad es. un esempio nel libro di Jean Tirole, *Economia del bene comune*, 2017 (orig.: 2016), Mondadori, cap. XIV, 405-428 nonché sinteticamente v. il suo *Market Failures and Public Policy*, § 3 *Two-Sided Markets*, discorso in occasione del ricevimetno del premio Nobel, reperibile in rete ad es. nel sito dell'ente erogatore www.nobelprize.org. Si ha una *multisided platform* quando <<*cross-platform network effects occur in at least one direction and the firm facilitates interactions between two or more groups of users, can set distinct prices to different user groups, and has market power with respect to those groups. Crossplatform network effects exist when the presence of members of group A as users on one side of the platform makes the platform more attractive to members of group B on another side*>> (Katz M.-Sallet J., *Multisided Platforms and Antitrust Enforcement*, cit., 2150, Prize Lecture, December 8, 2014). Tra i molti saggi in tena di *two-sided platforms* o *markets* v. R. Schmalensee-Evans D.S., *Industrial Organization of Markets with Two-Sided Platforms, in Competition Policy International*, Vol. 3, No. 1, Spring 2007, letto in ssrn.com, cap. I *Introduction i* e cap. II *Economic Background on Two-Sided Platforms*. Ora in termini accessibili v.: -Cohen J.E., *Between truth and power*, cit., 37-46 e 174-5; Franck J.U.-Peitz M., *Market Definition and Market Power in the Platform Economy*, Report May 2019 per *Centre on Regulation in Europe (CERRE)*, § 2.2; Rossi M.A., *Il ruolo delle piattaforme nell'economia dei big data*, in Falce V.-Ghidini G.-Olivieri G. (a cura di), *Informazione e big data tra innovaizone e concorrenza*, Giuffrè, 2018, p. 75 ss. Questo tipo di business crea qualche problema per l'applicazione delle categorie tradizionali antitrust, soprattutto nella individuazione del mercato rilevante: - Parikh S., *Defining the market for two-sided platforms: the scope of Ohio v. American Express*, in *Berk tech.law journ.*, 2019, vol. 34, 1305 ss., parte II, 1318 ss.; - Robertson V. H.S.E., *The EU's Attempt at Updating Antitrust Market Definition for the Digital Age*, in *promarket.org*, 21.07.2020; Lancieri F.-Sakowski P.M., *Competition in digital markets: a review of expert reports*, agosto 2020, Stigler Center of Chicago Booth School of Business, w orking Paper Series No. 303, parte IV-V; - Khan L.M., *Amazon's Antitrust Paradox*, in *Yale law journal*, 2017, vol. 126/3, 710 ss, parte II, sull'insufficienza dell'approccio di Chicago limitato al consumer welfare (condivisibilmetne, anche perché - come disse L. D. Brandeis- <<*we must make our choice. We may have democracy, or we may have wealth concentrated in the*

risposta al quesito diventa difficile. Provvisoriamente, però, direi che la ratio, sottostante al requisito del ruolo solo automatico e passivo del cons 42, dovrebbe essere rispettata anche nel caso di quelle attività lato sensu promozionali, che invece spesso inducono i giudici a ritenerlo violato, con negazione del safe harbour[119]. In altre parole, il provider

hands of a few, but we can't have both>>, ripreso dalla senatrice Warren E, *Questa lotta è la nostra lotta*, Garzanti, 2020, orig. 2017-2018, pp.209-210), parte III-IV sul business di Amazon e soprattutto parte V (pp. 784-790) sull'insufficienza di tale approccio per Amazon, che punta su un *quasi predatory pricing* (con forte riduzione dei profitti, assenti nei primi anni) e sulla diversificazione settoriale per diventare mezzo indispensabile per altre imprese (infine parte VI su due possibili interventi rimediali), come conferma l'ex *country manager* per l'Italia Angioni M., *Amazon dietro le quinte*, Raffaello Cortina Ed., 2020, passim ad es. 94, p. 173 ss. Il *recoupment* da parte di Amazon, dopo l'abbassamento dei prezzi, avviene non alzandoli in futuro, ma abbassando ulteriormente i costi variabili e facendo fruttare meglio quelli fissi (così Sussman S., *Prime Predator: Amazon and the Rationale of Below Average Variable Cost Pricing Strategies Among Negative-Cash Flow Firms*, in *Journal of Antitrust Enforcement*, Vol. 7/2, July 2019, 217, riportando dichiarazioni della stessa Amazon): in ogni caso, per l'a., essendo impossibile conoscere i costi di Amazon, i quali costituiscono il segreto più tutelato per qualunque impresa, è impossibile stabilire se ricorra *predatory pricing*. Mentre invece Amazon sa (quasi) tutto delle imprese presenti sul suo marketplace, per cui può operare discrminazioni e *information appropriation* concorrenzialmente asai dubbie: v. ampiamente Khan L., *The separation of platforms and commerce*, *Columbia law review*, 2019, vol. 119/4, passim, spt. I.A-I.D, 983 ss. (con riferimetno pure a Google Alphabet, Facebook e Apple), che poi (sub V) esamina i problemi di una possibile separazione tra l'attività sovraprofittevole e le altre per evitare che la prima sussidi le seconde, tenute magari sotto costo (anche se ciò non significa necessariamente separare l'attività di intermediario da quella di commerciante: p. 1070; intesssante rassegna delle ragioni alla base di passati scorpori a p.1052, sub IV). Attribuisce notevole importanza alla capacità di *storytelling* di Jeff Bezos (che gli permette di raccogliere finanziamenti a costi irrisori e con modeste distribuzioni di dividendi) il saggio di Galloway S., *The four. I padroni*, Hoepli, 2018, orig.: 2017, 31-33 (v. anche 36-39 e 174).

[119] Analoghe osservazioni in Wang J, *Regulating hosting ISP's responsabilities for coyright infringement. The freedom to operate in the US, EU and China*, Springer, 2018, sub 3.4, 62 ss. L'a. ricorda che in Cina il livello di duty of care degli ISP si innalza in presenza di situazioni in cui aumenta il rischio di violazioni e cioè: creazione di canali per film e serie TV, uploading di opere famose, opere visionate più di un certo numero di volte (ivi, 124 ss, sub 4.6). Se si conteggia l'interesse del provider nel trasmettere i contenuti circa la decisione sul safe harbour, allora per Google (circa il copyright) la situazione è ancora più "grave", anzi non c'è scampo, essendo quasi un *rule maker* più che *rule taker*: infatti <"*in this ecosystem of privacy copyright rule-making and enforcement Google is an ad apex predator. This is because Google owns and controls large portions of the internet but also because Google approach to copyright in practice can have the effect of "norm setting". (…). Google approach to copyright in practice has far*

indicizza e propone sì i file caricati dagli utenti, ma lo fa in modo massivo ed automatico, in base, da un lato, al tipo di contenuti presenti in detti file (rilevato da metadati, non da controllo dei fatti ivi rappresentati), e, dall'altro, alle preferenze rilevate dal tracciamento dati: analizza per ideal-tipi, cioè segmentando e categorizzando gli utenti[120]. In particolare non distingue (non può distinguere, direi) tra file a contenuto lecito e file a contenuto illecito[121], particolarmente laddove il giudizio dipende dal contesto[122]: il che è sufficiente per farlo rientrare nel concetto di safe harbour, emergente dal cons. 42[123]. E' vero che questo

reaching consequences. Google is a powerful decision-maker in digital copyright governance, capable of setting rules norms and standards that determine the scope and application of copyright law across large portions of the digital environment" (Gray J.E., *Google rules*, cit., 127). Il titolo del cap. 4 di Gray (*Innovate first, Permission later*, p. 65 ss), del resto, è assai significativo della sua forza; però in UE con la dir. 2019/790 è prevalsa l'industria culturale sul colosso di Mountain View.

[120] Delmastro M.-Nicita A., *Big data. Come stanno cambiando il nostro mondo*, Mulino, 2019, 37 (dividono in sei fasi il processo –circolare- di raccolta, analisi e successivo utilizzo dei dati).

[121] Conf. Geddes K., *Meet Your New Overlords: How Digital Platforms Develop and Sustain Technofeudalism*, cit., p. 469 e 476. Certamente non può distinguere per violazioni di IP, dato che potrebbe sempre esserci il consenso o almeno la tolleranza del titolare o ricorrere altre difese (in USA, fair use; da noi quelle ex art. 5 dir. 2001/29 oppure ex art. 65 ss. l. aut.). Meno lineare è la situazione per violazioni di diritto della personalità, che potrebbero essere ritenuti non disponibili: ma anche qui il caricamento da aprte dei titolare (diffamato, bullizzato etc.) può essere escluso in assoluto, ad es. quando egli vuole dimostrare a quali vergognoso trattamenti è stato sottoposto? Del resto anche la *manual moderation* è di qualità assai bassa: DeLisa N.T., *You(Tube), Me, and Content ID: Paving the Way for Compulsory Synchronization Licensing on User-Generated Content Platforms*, 81 *Brooklyn Law Review*, (2016), pp. 1293-1294.

[122] Bloch-Wehba H., *Automation in Moderation*, 2020, *Cornell International Law Journal*, Forthcoming, leggibile in https://ssrn.com/abstract=3521619, p. 29/30 del.pdf.

[123] Simile considerazione nelle Conclusioni 22.09.2009 dell'AG Pojares Maduro in *Google France c. Louis Vuitton*, cause riunite C-236/08, C-237/08 e C-238/08: <<*Questo punto è meglio illustrato dal confronto con il motore di ricerca della Google, che è neutro rispetto alle informazioni che trasmette (72). I suoi risultati naturali sono il prodotto di algoritmi automatici che applicano criteri oggettivi per generare siti di probabile interesse per l'utente di Internet. La presentazione di tali siti e l'ordine in cui vengono visualizzati dipende dalla loro pertinenza alle parole chiave immesse, e non dall'interesse della Google in specifici siti o dal suo rapporto con i medesimi. È vero che la Google ha un interesse – e anche pecuniario – a presentare all'utente di Internet i siti maggiormente pertinenti; tuttavia, essa non ha alcun interesse a portare all'attenzione di detto utente un sito specifico*>>, § 144.

trattamento di dati, proprio perché opera un *matching* tra i due lati del mercato (preferenze dei navigatori vs. proposte commerciali degli inserzionisti) può dirsi che lo faccia in base ai contenuti, su cui vengono lasciate tracce dai navigatori: ma appunto si tratta –a quanto risulta- di tracce abbinate a parole chiave, abstract o altri parametri sintetici, prefissati per ciascun prodotto/file visionato[124]. E' certo che, purtroppo, le piattaforme non hanno alcun incentivo a ridurre i contenuti socialmente pericolosi[125]: ma ciò è altro dalla conoscenza dell'illecito via via sub iudice, che preclude la fruizione del safe harbour..

Secondo la Commissione UE, del resto, l'organizzazione e promozione dei file costituisce indice del requisito di <funzionalità essenziale> per integrare il concetto di <piattaforma per la condivisione video>, secondo l'importante dir. 2018/1808 di modifica della dir. sui servizi di media audiovisivi[126] (che richiederebbe esame specifico). E' dunque il

[124] Riordan J., *The liability of internet intermediaries*, cit., 401-401, applica il safe harbour a queste attività, stante la loro tecnicità ed automaticità, per cui può dirsi che siano applicate *neutrally*.

[125] Si v. la sopra accennata *stickiness* e la relativa chiosa di Khan L.M.-Pozen D.E., *A Skeptical View of Information Fiduciaries*, in *Harvard law review*, vol. 197, 10 Dic. 2019, p. 505-506: "*By and large, addictive user behavior is good for business. Divisive and inflammatory content is good for business. Deterioration of privacy and confidentiality norms is good for business. Reforms to make the site less addictive, to deemphasize sensationalistic material, and to enhance personal privacy would arguably be in the best interests of users. Yet each of these reforms would also pose a threat to Facebook's bottom line and therefore to the interests of shareholders*". Anche volessero tale riduzione, poi, c'è il problema per cui con il machine learning gli output non sono del tutto predefinibili (per definizione): notazione comune, ma v. ad es. la trascrizione dell'audizione dello scienziato computazionale anglo-statunitense Stephen Wolfram al Senato USA, *Optimizing for Engagement: Understanding the Use of Persuasive Technology on Internet Platforms*, 25 giugno 2019 (ove si legge ad es. <<*But as a matter of principle, it means that it can ultimately be impossible to completely verify that a program is "correct", or has some specific property.Software engineering has in the past often tried to constrain the programs it deals with so as to minimize such effects. But with methods like achine learning, this is basically impossible to do. And the result is that even if it had a complete automated content selection program, one wouldn't in general be able to verify that, for example, it could never show some particular bad behavior*>>, p. 7; scritto molto interessante).

[126] Comunicazione 07.07.2020 *Orientamenti relativi all'applicazione pratica del criterio di funzionalità essenziale della definizione di «servizio di piattaforma per la condivisione di video» a norma della direttiva sui servizi di media audiovisivi* (2020/C 223/02), sub III.1, III.3 e III.IV, a proposito del cons. 5 della dir. 2018/1808 e del nuovo art. 1 § 1 lett. a bis) della dir. 2010/13. A dire il vero nel secondo si parla di *obiettivo principale: <<ove l'obiettivo principale del*

tipo di business ad imporre queste modalità operative, a prescindere da qualunque partecipazione allo specifico illecito sub iudice. La dir. 2018/1808 sembra dare per scontato che simili piattaforme, in linea di massima comprendenti pure i social media[127], non abbiano responsabilità editoriale: dice infatti di applicarsi ai servizi offerti da simili piattaforme, <per i quali [servizi] il fornitore della piattaforma per la condivisione di video non ha responsabilità editoriale> (art. 1, che introduce l'art. 1 § 1 lett. a bis) nella dir. 2010/13). Teoricamente, o meglio letteralmente, potrebbe obiettarsi che la disposizione si limitasse a delimitare il proprio campo di applicazione ai servizi, per i quali la piattaforma non abbia responsabilità editoriale, impregiudicata l'esistenza di piattaforme che invece l'abbiano. Effettivamente la disposizione è ambigua, non chiarendo come vada dato il giudizio sulla presenza/assenza di responsabilità editoriale, in particolare se su base soggettivo/volontaristica (scelta, esplicita o implicita, della piattaforma) oppure oggettiva (in tale caso, su quale parametro): parrebbe esatta la seconda alternativa, anche alla luce del precedente (e in pratica contrapposto) concetto di <servizio di media audiovisivi>, che ricorre quando l'obiettivo principale <<sia la fornitura di programmi al grande pubblico, sotto la responsabilità editoriale di un fornitore di servizi di media, al fine di informare, intrattenere o istruire, attraverso reti di comunicazioni

servizio stesso, di una sua sezione distinguibile o di una sua funzionalità essenziale sia la fornitura di programmi>>, il che non è ben coordinato col predetto cons. 5: che la condivisione di UGC sia l'obiettivo principale di una funzionalità essenziale del servizio di *video-sharing* non è uguale –almeno letteralmente- al dire che la convisione di UGC costituisca la funzionalità essenziale del servizio offerto dalla piattaforma (nel primo caso possono esserci altre funzioalità essenziali, che offrono utilità del tutto diverse, mentre il secondo caso presuppone una sola funzionalità essenziale, quella di condivisione di UGC). Non accenna alla distinzione Kuklis L., *Media regulation at a distance: video-sharing platforms in Audiovisual Media Services Directive and the future of content regulation*, Riv. dir. media, 2020/2, medialaws.eu, 98.

[127] v. Cons. 4 dir. 2018/1808: <<*Ciò vale anche per i servizi dei media sociali, che sono diventati un importante mezzo per condividere informazioni, intrattenere e istruire, anche dando accesso a programmi e video generati dagli utenti. Tali servizi di media sociali devono essere inclusi nell'ambito di applicazione della direttiva 2010/13/UE perché sono in concorrenza con i servizi di media audiovisivi per lo stesso pubblico e le stesse entrate. Inoltre, hanno anche un impatto significativo in quanto facilitano la possibilità che gli utenti modellino e influenzino i pareri di altri utenti.*>>.

elettroniche>> (art. 1, di modifica dell'art. 1 § 1 lett. a) della dir. 2010/13). Ad ogni modo, in base alla disposizione cit., è probabilmente legittimo dire che "di solito" le piattaforme ospitanti video degli utenti, pur se arricchite da organizzazione attiva e non solo passiva, sono prive di responsabilità editoriale. Pare allora azzardato privare del safe harbour simili piattaforme quando esse, per il legislatore, di solito non hanno responsabilità editoriale[128].

Del resto la C.G. esclude la legittimità di inibitorie preventive, che richiedano monitoraggio esteso, laddove rischino <<*di ledere la libertà di informazione, poiché tale sistema potrebbe non essere in grado di distinguere adeguatamente tra un contenuto lecito ed un contenuto illecito, sicché il suo impiego potrebbe produrre il risultato di bloccare comunicazioni aventi un contenuto lecito. Infatti, è indiscusso che la questione della liceità di una trasmissione dipende anche dall'applicazione di eccezioni di legge al diritto di autore che variano da uno Stato membro all'altro. Inoltre, in certi Stati membri talune opere possono rientrare nel pubblico dominio o possono essere state messe in linea gratuitamente da parte dei relativi autori*>>[129]. Ebbene, il non poter distinguere tra lecito e illecito, se osta a tale dovere di monitoraggio, è coerente ritenere che osti pure alla perdita del safe harbour: come non può rischiare di conculcare la libertà d'espressione degli utenti, così pure non può rischiare di conculcare il diritto al safe harbour degli internet provider. I diritti dei primi non sono maggiori in parte qua di quelli dei secondi, i cui servizi sono pure essenziali per la collettività[130].

Il che vale a maggior ragione, se si considera che gli algoritmi,

[128] Secondo il cons. 48 dir. 2018/1808, le misure protettive per il pubblico, gravanti sulle piattaforme di video-sharing, <<*dovrebbero riguardare l'organizzazione dei contenuti e non i contenuti in quanto tali*>>. Il medesimo cons. 48, poi, fa salvo il safe harbour ex dir. 2000/31 e quindi pare considerarlo prevelente in caso di contrasto con la dir. 2018/1808: a parte altre osservazio0ni sistematiche, però, la sua collocazione tra i considerando priva questa importante "regola" di precettività: se avesse voluto invece conferirgliela, il legislatore avrebbe dovuto inserirla nell'articolato.

[129] C.G. 24.11.2011, Scarlet Extended c. SABAM, C-70/10, § 52.

[130] Sopratutto alla luce della tragedia sanitaria che ha colpito tutto il mondo alla fine dell'inverno 2019-2020. Del resto ritenere sufficiente il *general intent*, anziché lo *specific intent to induce*, per gravare gli ISPs di secondary liability, rischia di inibire lo sviluppo di utili servizi e tecnologie internet (Wang J., *Regulating hosting ISP's responsabilities*, cit., 130-132).

governanti questi processi economici, son sempre più capaci di autoapprendimento (*machine-learning*, soprattutto le c.d. *deep neural networks*): con la conseguenza che i risultati vengono ottenuti da modelli (patterns) che nemmeno i progettisti riescono a spiegare (o non in toto)[131]. Essi non predicono il futuro, ma - in base ai dati esistenti - stimano le probabilità che qualcosa accada[132]. Per cui in tali casi non si può più parlare di "conoscenza o controllo delle informazioni trasmesse o memorizzate": a meno di imputare queste in via oggettiva, esito però (forse astrattamente plausibile, ma) in concreto difficilmente accoglibile, senza una norma ad hoc, visto il tenore del cons. 42, e sempre che gli sia dia l'importanza ermeneutica (decisiva), che gli danno i sostenitori della distinzione provider

[131] Molta letteratura in merito. Si v. ad es. - Bathaee Y., *The artificial intelligence black box and the failure of intent and causation*, in *Harvard Journal of Law & Technology*, 2018, Vol. 31/2, 889 ss, passim (spt. 891 e parte II, 897 ss), che ne esamina poi le ricadute sull'elemento soggettivo e sul nesso di causalità nell'illecito; più brevemente, Brauneis R.-Goodman E.P., *Algorithmic Transparency for the Smart City*, *Yale Journal of Law & Technology*, 2018, vol. 20, 103 ss a 131-132; Nicholas G., *Explaining algorithmic decisions*, in *Gergetown law technology review*, vol. 4/2, 2020, p. 714. Tuttavia il grado di impenetrabilità e inesplicabilità non è sempre uguale, dipendendo dalla complessità del modello e dal training iniziali: - Hilty R., Hoffmann J., Scheuerer S., *Intellectual Property Justification for Artificial Intelligence*, Max Planck Institute for Innovation and Competition, Research Paper No. 20-02, 2020, letto in ssrn.com, 8; - Drexl, Hilty et al., *Technical Aspects of Artificial Intelligence: An Understanding from an Intellectual Property Law Perspective*, Version 1.0, October 2019, Max Planck Institute for Innovation and Competition Research Paper No. 19-13, letto in ssrn.com.; Relazione del Parlamento Europeo recante *raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica* (2015/2103(INL)) del 27.01.2017, sub *Responsabilità.AA* (sulla modulabiltià dell'autonomia del robot); - Nicholas G., *Explaining algorithmic decisions*, cit., p. 726/7 (l'inesplicabilità aumenta quando più algoritmi vengano in vario modo fatti funzionare assieme, c.d. *ensemble methods*). Naturalmente i problemi maggiori delle black box riguardano il difetto di trasparenza, che rende assai difficile verificare il rispetto delle regole governanti sia i rapporti privatistici (soprattutto la buona fede in tutto il ciclo contrattuale: formazione ed esecuzione), sia l'azione ammninistrativa nei rapporti pubblicistici (sul noto caso degli "errori" compiuti dall'algoritmo nell'assegnazione delle cattedre ai docenti, deciso da Cons. Stato, VI, 13.12.2019, n. 8472-8473-8474, sono già intervenuti molti commenti: ad es. v Muciaccia N., *Algoritmi e procedimento decisionale: alcuni recenti arresti della giustizia amministrativa*, www.federalismi.it, 15.04.2020, n. 10/2020).

[132] Così Waldman A.E., *Power, Process, and Automated Decision-Making*, 88 Fordham L. Rev. 613 (2019), p. 617. Per l'a. il ricorso diffuso alle decisioni algoritmiche rappresenta una forma di policymaking neoliberale (p. 624 ss).

attivo/provider passivo[133].

Questo modus operandi allora non pare costituire "conoscenza delle informazioni trasmesse o memorizzate" ex cons. 42: non solo o non tanto perché sia automatizzato[134], quanto –ancor prima- perché la conoscenza, che serve ai grossi provider e quindi quella effettivamente raccolta nell'organizzare e proporre i file, è solo quella finalizzata a creare gli abbinamenti più compatibili (e quindi sperabilmente più desiderabili e fruibili) con le tracce delle fruizioni pregresse. Non è lontana da questa posizione quella di chi sostiene che la ratio del requisito di passività stia nel tracciare una linea divisoria tra materiali propri (o fatti propri, "adopted content", come per la responsabilità editoriale) e materiali altrui (third-party information), anziché nel restringere il safe harbour[135].

Proprio sulla difficile applicabilità a sé di questa distinzione gioca Facebook: da un lato pretende di non essere responsabile per l'illiceità dei materiali caricati dagli utenti, in quanto non propri, e dall'altro invoca però la freedom of speech di cui al Primo Emendamento (<<*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press;* …>>)[136]: la quale però gli spetterebbe solo se avesse appunto

[133] Tesi ermeneutica da scartare, come visto, dal momento che la regola è rimasta confinata nei considerando, senza entrare nell'articolato della dir.: come avrebbe dovuto, stante sia la sua importanza che la sua lontananza (non desumibilità) dal dettato degli artt. 12-15 dir.

[134] Teoricamente può esserci (anzi, già ci sarà) un automatismo pure nella assimiliazione completa dei contenuti: probabilmente si può pensare al software Watson di IBM (https://en.wikipedia.org/wiki/Watson_(computer)).

[135] M. Husovec, *Injunctions aganist intermediaries*, cit., 55-57 che cita come esprimente lo stesso principio la conclusioni di AG Szpunar in Ziggo –Piratae Bay, C-610/15, § 53. Qui però l'AG afferma si che serve la consapevolezza dell'operatore ma per la violazione di diritto d'autore (comunicazione al pubblico) (si v. §§ 48-54): che è cosa diversa dalla questione della fruizione del safe harbour. L'influenza del *modus operandi* delle piattaforme sui mezzi di informazione tradizionali è esaminata nell'interesante saggio di Carroll E.C., *Platforms and the Fall of the Fourth Estate: Looking Beyond the First Amendment to Protect Watchdog Journalism*, cit., p. 565 ss sub B (per l'a. le piattaforme svoltono un ruolo editoriale: "*No matter how vehemently they deny it, platforms are playing press roles. Manipulating the algorithms that surface content is an editorial act*", p. 577).

[136] v. la voce *First Amendment to the United States Constitution* in *Wikipedia*. Il riferimento al Primo Emendamento domina le ricerce su *free speech* e termini concettualmente prossimi (First Amendment, free speech, free expression,

responsabilità editoriale e cioè se creasse un proprio <*expressive speech*> [137]. Di recente ha leggermente modificato (rectius: ha dichiarato di aver leggermente modificato) l'algoritmo per il newsfeed, incrementando le "*meaningful social interactions*" e retrocedendo i post imprenditoriali, di marchi commerciali e di mass media, per favorire il people well-being, pur se meno redditizio per la piattaforma. In realtà l'ha verosimilmente fatto soprattutto per ridurre il rischio di perdere il safe harbour posto dal (per lei utilissimo) § 230 CDA[138]: e ciò sia riducendo il focus sul suo ruolo editoriale (che risalta di più nei contenuti spinti da Facebook rispetto a quanto avviene per quelli condivisi da familiari e amici), sia sviando l'attenzione pubblica (soprattutto di politici, giudici e pubblico in genere) dalla necessità di modifica del citato safe harbour[139] (opzione recentissimamente

freedom of speech, freedom of expression): v. il grafico tratto da Google Ngram Viewer cit. da Gordon J.S., *Silence for sale, Alabama law rebiew*, vol. 71/4, 2020, p. 1159 (approfondito saggio sui *non disclosure agreement-NDA*, assai diffusi in USA: l'a. sostiene l'opportunità di una loro maggior impugnabilità rispetto a quanto ammette la giurisprudenza, rigorosamente ancorata al formale principio della libertà contrattuale, nei fatti spesso ridotta o assente).

[137] Halsey A., *ISPs Want to Have Their First Amendment Cake and Eat it Too*, in *publicknowledge.org*, 20.08.2010; Thompson K.A., *Commercial Clicks: Advertising Algorithms as Commercial Speech*, cit., 1035; Zuboff S., *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri,* LUISS Univ. Press, 2019, 120.

[138] Interessant report sulle applicazioni giudiziali del § 230 CDA in Banker E. (per Internet Association), *A Review Of Section 230's Meaning & Application Based On More Than 500 Cases*, 27 luglio 2020, internetassociation.org (ove si legge che non sono solamente le grandi piattaforme ad invocarla: v. Finding 1).

[139] Sulle possibilità di modifica (leggi: restrizione) del safe harbour ex § 230 CDA, tra i moltissimi v.:- Keller D., *Toward a clear covnersation about platform liability*, in Pozen D.E. (a cura di) *The perilous public square*, cit., p. 210 ss., cautamente favorevole, ove anche breve sintesi degli argomenti favorevoli e contrari; Lagg E., *Stormy Waters for the Internet's Safe Harbor: The Future of Section 230*, 71 Rutgers U.L. Rev. 763 (2019), p. 780. L'a. allo stesso scopo suggerisce alla piattaforma di continuare ad usare le denunce degli utenti come mezzo principale per individuare e rimuovere i post illeciti, soprattutto sulla base della decisione *FTC v. LeadClick Media, LLC* del 2016 (p. 776-779); - Skorup B.- Huddleston J., *The Erosion of Publisher Liability in American Law, Section 230, and the Future of Online Curation*, 72 *Okla. L. Rev.* 635 (2020), sub III: per gli aa l'eventuale responsabilità dovrebbe limitarsi ai casi, in cui <<*(1) there is general agreement that the content at issue has minimal speech value, (2) where basic software programs or nonexpert curators can easily identify the content as impermissible, and (3) dedicated content removal efforts would have a limited impact on legitimate speech*>> (ivi, p. 661); - Volpe B., *From Innovation to Abuse: Does the Internet Still Need Section 230 Immunity?*, 68 Cath. U. L. Rev.

attuata dal Presidente Trump tramite un suo executive order del 28 maggio 2020, a seguito della polemica con Twitter)[140].

8. Non necessità del requisito di passitivà (pur con qualche dubbio)

la conclusione suggerita potrebbe tuttavia sembrare opinabile, se uno applica il requisito di passività previsto dal cons. 42 pure all' hosting provider: dato il pesantissimo intervento degli algoritmi nel determinare ciò che gli utenti "vedono", può diventare difficile ritenere "neutre e passive" le piattaforme che li usano[141]. Non resterebbe forse che un argomento teleologico, accennato sopra: il design dell'algoritmo è si determinante per newsfeed e SERP, ma per motivi diversi e non connessi con l'illecito sub iudice e con i contenuti illeciti in generale. Potrebbe obiettarsi che i contenuti illeciti, se fanno comodo alla piattaforma in termini di spazi pubblicitari (probabilmente è così, dato che i relativi fruitori saranno fruitori anche dei contenuti analoghi), la piattaforma è ben contenta di

597 (2019), suggerendo l'introduzione di un meccanismo di responsabilità a seguito di inottemperenza a diffida come nel § 512 DMCA e nel safe harbour europeo (ivi, sub IV.A, p. 619-620). Contraria ad abrogazione e modifiche, invece, è Wiener A., *Trump, Twitter, Facebook, and the Future of Online Speech*, in *The New Yorker*, 06.07.2020.

[140] v. la notizia nel sito della Casa Bianca ; Facebook parrebbe invece intenzionata a tenersene fuori (Isaac M.-Kang C., *While Twitter Confronts Trump, Zuckerberg Keeps Facebook Out of It*, The New York Times, 29 maggio 2020, edizione online). Tale *order* presidenziale, dopo un peana alla libertà di espressione che viene inibita dalla censorship esercitata dalle piattaforme (Sec. 1 *Policy*), incarica la Federal Communications Commission (FCC) di proporre modifiche legislative, per restringere l'immunità offerta dall'attuale § 230 CDA (Sec. 2.(a) e soprattutto Sec. 2.(b)). Il Presidente invoca (Sec. 4(a)) l'autorità dei casi *Packingham v. North Carolina* e *Prune Yard Shopping Center v. Robins*, qui citati. Un primo inasprimento del safe harbour è stato introdotto nel 2018 la c.d legge SESTA/FOSTA (dagli acronimi di due progetti di legge poi fusi: il *Allow Victims and States to Fight Online Sex Trafficking Act -FOSTA-* e *Stop Enabling Sex Trafficking Act –SESTA-*) che ha abrogato il safe harbour per i reati ivi indicati, aggiungendo la lettera (e) al § 230 CDA: tra i molti aa., v. McKnelly M., *Untangling SESTA/FOSTA: how the internet's "knowledge" threatens anti-sex trafficking law*, in *Berkeley technology law journal*, vol. 34/3, aprile 2020, 1239 ss, a p. 1251 e 1253.

[141] Per questo motivo, secondo taluni a. già *de iure condito*, queste piattaforme non sono protette dal § 230 CDA, voluto quando l'attuale modo di gestire gli UGC non era ancora all'orizzonte: Sylvain O., *Intermediary Design Duties*, 50 Conn. L. Rev. 203 (2018), passim ad es. pp. 214-215

riproporli[142]. Questa è però una considerazione di buon senso, che difficilmente costituisce prova sufficiente –nemmeno argomento di prova- sia ai fini della concessione del safe harbour, sia (in positivo) ai fini dell'affermazione di responsabilità: da un lato, è mera illazione e, dall'altro, in entrambi i casi è richiesto uno stato soggettivo relativo allo specifico illecito sub iudice anziché in astratto (a differenza del mere conduit, come visto)[143]. Per cui bisognerebbe conoscere ed

[142] Affronta il punto Sylvain O., *Intermediary Design Duties*, cit., sub I.C, p. 226 ss (§ titolato *antisocial design*): la politica di Facebook, per contrastare gli inserzionisti che usano criteri illeciti (discriminatori) nel loro advertising, *is either naive or careless or worse*, visto che è lei stessa ad offrire tali possibilità di mictotargeting (p. 230). Osservazione ineccepibile, direi. V. poi lì'ampio saggio di Lavi M., *Do platforms kill?, Harvard Journal of Law & Public Policy*, 2020, vol. 43/1, 477ss., centrato sul contrasto alla propaganda terroristica: <<*although it may appear that the system operates without human intervention, the intermediary structures it and the operation of the algorithm depends on the discretion of its programmers who can program it without neutrality or tinker with the results ex post.. Algorithms are also never truly neutral. This practice of algorithmic-based recommendations and targeting can influence users' future choices and the likelihood of changing their minds. This influence may be positive or negative. Beyond the general risk of infringement on users' autonomy and the risk of shackling them to their past interests and decisions, intermediaries can present harmful content to specific users through an automated recommendation system*>> (p. 502/3) e poi sub III.B.1, spt. p. 531, ove si legge che <<*the ability of the intermediary to predict and influence users' behavior as a means to produce revenues raises a red flag. Intermediaries' liability for targeting can be justified to promote public safety. The chilling effect on recommendations is expected to be proportional because the intermediary can design the platform to avoid targeting unlawful content*>>. E ancora: <<*by targeting content, the intermediary's algorithm not only repeats the content of users and advertisers, but also selects content for publication and displays different types of content to different audiences. By doing so, the intermediary influences the context of the content and the magnitude ascribed to it. Therefore, intermediaries that design platforms and their code can be held responsible, at least in part, for creating or developing content. This approach can be applied to algorithmic recommendations and targeting in particular*>> (p. 546). Per cui l'immunità ex § 230 CDA non si applica (ivi, p. 547).

[143] Sulla stessa linea di pensiero v. ora le conclusioni 16.07.2020 dell'§AG Saugmandsgaard ØE in C.G., C-682/18 e C-683/18, *Peterson c. Google-Youtube e Eelsevier c. Cyando*, alla sez. 3.B (seconda questione pregiudiziale, *The field of application of the exemption from liability under Article 14(1) of Directive 2000/31*), spt. § 150-168: il ruolo attivo che esclude il safe harbour deve essere tale da far apparire lo specifico contenuto come proprio o sotto il controllo della piattaforma (*deemed to acquire intellectual control of that content/ dass er die geistige Herrschaft über diesen Inhalt erwirbt*), sicchè non ricorre nei due casi sub iudice. Analoga risposta dà l'AG circa lo stato soggettivo di conoscenza riccheisto dalll'art. 14 § 1 lett. a dir. 2000/31: <<*In essence, the question is whether, in order*

analizzare l'algoritmo, per accertare se si potesse ravvisare difetto (per colpa o dolo eventuale) nella sua progettazione complessiva: che a questo punto diverrebbe un prodotto difettoso, fonte di danni per i terzi che vengano in contatto con esso[144]. Ma ci sarebbero serissimi problemi nell'accesso all'algoritmo nella probabile (quasi certa) ipotesi, in cui il titolare del diritto d'autore su di esso si rifiutasse di ostentarlo (anche solo in giudizio): da un lato, l'art. 210 c.p.c. riguarda "cose" e, dall'altro, notoriamente la sua inottemperanza è priva di sanzione (a parte la ravvisabilità di argomenti di prova ex art. 116 c.2 c.p.c.)[145].

Il punto è ad es. al centro dell'attenzione di saggi recenti, secondo cui la progettazione e in generale il modo di funzionare

to deny the provider concerned the benefit of the exemption under Article 14(1) of Directive 2000/31, the applicant must show that the provider had 'knowledge' or 'awareness' of that information in particular or whether it need only demonstrate that the provider had general and abstract 'knowledge' or 'awareness' of the fact that it stores illegal information and that its services are used for illegal activities. In my view, the situations referred to in Article 14(1)(a) of Directive 2000/31 actually relate to specific illegal information.>> § 171-172 (e v. pure § 185; ma si v. tutta la sez. 3.C dal § 169 in poi). V. pure l'interessante precisazione, per cui, dopo la notifica, il provider deve procedere a rimozione/disabilitazione ma non è tenuto a prevenire un futuro re-uploading: per cui va respinta l'istanza dei titolari, che interpretano l'article 14(1) della dir. 2000/31 <as underlying a system not merely of notice and take down, but notice and stay down.>, § 193.

[144] L'aver progettato un algoritmo che permette o favorisce certe condotte illecite (tipologicametne individuate) probabilmente costituirebbe negligenza o dolo (eventuale) anche relativamente a quella concreta sub iudice: accettare o favorire una classe di eventi, infatti, vuol dire accettare o favorire anche ciascuno di essi singolarmente considerato. La categorizzazione (profilazione, *social sorting*) è alla base della gestione dei *big data* (Lyon D., *La cultura della sorveglianza*, passim, ad es. pp. 33, 37, 44, 83-86 per il software Zodiac dei supermercati inglesi Tesco ed altri esempi reali, pp.92/3, p. 113 ss., p. 188 ss.) e va di pari passo con (anzi è inseparabile dal-) la sorveglianza (Lyon D., ivi, 105).

[145] Sarebbe poi interessante esaminare un'ipotetica difesa del titolare dell'algoritmo che, a parte quanto affermato nel testo, sostenesse che la sua divulgazione anche solo processuale è inconciliabile col fatto che si tratta di privativa intellettuale protetta (anche solo come segreto aziendale), la quale, se rivelata, di fatto metterebbe in serio (forse mortale) pericolo il business aziendale. Discute se il danno da A.I. nelle cure sanitarie (telehealth e telemedicine) generi responsabilità da prodotto difettoso (in quanto *medical device*) oppure da *medical malpractice* (in quanto *medical procedure or service*), Alshanteer M., *A current regime of uncertainty: improving assessments of liability for damages caused by artificial intelligence*, in *North Carolina J. of law & tech*., vol. 21/4, 2020, 27 ss., soprattutto sub IV.A, p. 42 ss (rilevandone applicazioni giudiziali incoerenti e fonto di incertezza).

degli algoritmi di oggi son assai più complessi e assai più determinanti della diffusione dei contenuti ricevuti, rispetto a quelli diffusi nel 1996 (anno del § 230 Communications Decency Act, di seguito solo: § 230 CDA): per cui i provider che li usano non son più necessariamente protetti da tale ombrello, dato che possono diventare in tal modo responsabili o corresponsabili <<for the creation or development of information>> e dunque diventare content provider (§ 230.f.3 CDA) [146], sostanzialmente tramite la fine granularità (elevato

[146] Sylvain O., *Discrminatory designs on user data*, in Pozen D.E. (a cura di) *The perilous public square*, cit., 181 ss e soprauttutto 189 ss. e più distesamente in Sylvain O., *Intermediary Design Duties*, cit., parte III a 258 ss sullo stato dell'arte (ove soprattutto v. l'importante sentenza *Fair Housing Council of San Fernando Valley v. Roomates.com* del 2008) e parte IV p.269 ss. sulla posizione dell'a. Nell'ultima parte del saggio l'a. contesta che possa applicarsi l'immunità a Facebook per le violazioni delle leggi antidiscriminatorie, dato che i dati raccolti –di per sé non dscriminatori e dunque lecitamente raccolti- permettono però agli inserzionisti di fare advertiging discrminatorio (ivi, p. 272 ss; l'a. riprende il tema sul *New York Times* del 28 marzo 2019 con *A Watchful Eye on Facebook's Advertising Practices*). Nello stesso senso: - Kim P. T., *Manipulating Opportunity*, in *Virginia Law Review*, Vol. 106, 2020, IV.A, p. 919-929, passim, per cui: i) nell'advertising generale si fuoriesce dall'ambito applicativo del § 230.(c).(1) CDA, trattandosi di violazione procedurale invece che contenutistica e dunque esulante in toto dal concetto di speaker e di publisher; ii) nell'advertising delle offerte lavorative la piattaforma diventa addirittura content provider; - Overton S., *State Power to Regulate Social Media Companies to Prevent Voter Suppression*, in *U.C. Davis law review*, 2020, vol. 53, 1793 ss., sub II.A e II.B, 1812 ss.; Byrd M.-Strandburg K.J., *CDA 230 for a Smart Internet*, 88 Fordham L. Rev. 405 ss. (2019): per le aa. Facebook viola la disciplina antidicrminatoria e spt. il Fair Housing Act (sub III, 415 ss) né può fruire del § 230 CDA vuoi perché non rientrante nel concetto di *publisher* (sub IV.A) vuoi perchè *information content provider* per la selezione sia dei destinatari *Attribute-Based* (sub IV.B.1) sia di quelli "simili" (*Lookalike Audience*, sub IV.B.2), ammettendo però che reali chances di successo in corte esistono solo per l'ultimo aspetto (p. 428/9); - tendenzialmente pure Lobel O., *The Law of the Platform*, cit., sub IV.B., p. 144-146 (letto in ssrn.com). Questa nuova pratica di advertising è invero seguita da molte altre piattaforme, dato che tutto il microtargeting funziona così. Il rischio di discrminazioni nelle offerte commerciali su piattaforme digitali è del resto un dato segnalato da molti: v. ad es. Cahn N.-Carbone J.-Levit N., *Discrimination by Design?, Arizona state law journal*, 2019, vol. 51/1, 1 ss.. La discplina posta dal § 230 CDA, anzi l'interpetazione estesa dell'immunità da essa ricavata dalle Corti USA, è oggetto di molte critiche, per le quali le Corti medesime si sarebbero troppo allontanate dalle intenzioni del legislatore storico: ad es. v. Graw Leary M., *The Indecency and Injustice of Section 230 of the Communications Decency Act*, 41 Harv. j. l. & pub. policy, 553 (2018), sub III.A, p. 573 ss. (la quale pure ricorda il caso *Fair Housing Council of San Fernando Valley v. Roomates.com* come esempio di corretta applciazione del § 230, p.576/7); oppure Kosseff J., *The Twenty-Six Words That Created the Internet*, Cornell Univ. Press, 2019, part III,

dettaglio) delle opzioni di scelta possibili agli utenti. La considerazione è interessante, ed è supportata pure da analisi tecniche[147], solo che si basa su una disposizione che da noi non esiste: da noi, per fruire del safe harbour, basta che il provider non sappia dell'illiceità portata dai file ospitati o che, se sa, provveda subito alla rimozione/disabilitazione[148]. Pertanto, ad una prima riflessione, non pare desumibile dal dettato normativo esistente. Né dall'art. 14 dir. 2000/31 § 1, laddove richiede che si tratti di informazioni fornite dal suo cliente (quindi non in proprio): indubbiamente i file illeciti sono caricati proprio dal cliente della piattaforma. Né dall'art. 14 dir. 2000/31 § 2, non potendosi dire che organizzare e proporre file alla fruizione di possibili interessati equivalga a diventare content provider.

Si potrebbe insistere nella linea qui avversata (ma fatta propria dalla maggior parte di giurisprudenza e dottrina), dicendo che anche solo il proporre quanti più file possibile incrementa la possibilità di downloading (anche) di quelli illeciti e quindi il rischio di violazioni. Anzi, visto che il diritto è governo di conflitti reali, dicendo che nel caso specifico le proposte della piattaforma hanno contribuito alla violazione dello specifico diritto azionato. Tuttavia l'allegazione del

165 ss,, soprattutto per la forza dell'importante precedente *Zeran v. America Online* del 1997 (qui trovi una dettagliata esposizione storica della nascita -parte I e II- e dell'applicazione del § 230 (parte III), oltre che delle sue prospettive di riforma (parte IV).

147 V. Ali M.-Sapiezynski P.-Bogen M.-Korolova A.-Mislove A.-Rieke A., *Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes*, 12.09.2019, (manoscritto non pubblicato e visto citato in Byrd M.-Strandburg K.J., *CDA 230 for a Smart Internet*,, cit., nota 5), spt. *Introduction* a p. 2-3 e *Policy Implications* a p. 14-15. Gli aa. riferiscono degli esperimenti condotti, dai quali si ricava il contributo decisivo dell'algoritmo di Facebook nel produrre gli esiti discriminatori nella delivery della pubblicità, imprevedibili anche agli stessi inserzionisti (conclusione tutt'altro che strana, peraltro). Per una descrizione del funzionamento dell'advertising su questa piattaforma v. ivi, sub 2 *Background*). Levy K.-Barocas S., *Designing aganist discrimination in online markets*, in *Berkeley technology law journal*, 2017, vol. 32, 1184 ss, a 1192 ss., individuano dieci tipi di modalità, raggruppabili in tre macrocategorie (1) setting platform- and community-wide policies; 2) structuring users' encounters and experiences on the platform; 3) monitoring and evaluating platform activity to root out bias e cioè i ratings), con cui il design delle piattaforme esaminate (oltre cinquanta) incide sulle possibilità discriminatorie.

148 Inoltre il § 230 CDA, sub (e).(2), fa salva l'applicazione dell' intellectual property law e cioè del § 512 DMCA, il quale ha costituito il modello del safe harbour europeo.

contributo all'aumento di rischio di violazione non pare pertinente: non è questo che (non solo nell'art. 14 d dir. 2000/31 ma nemmeno) nel cons. 42 osta al safe harbour.

Del resto e passando alla responsabilità in positivo (anziché solo in negativo, come proprio del safe harbour)[149], l'incremento del rischio di violazioni pare irrilevante pure ai fini del giudizio di responsabilità (aquiliana, precedendo l'avviso): il soggetto leso, infatti, dovrebbe dimostrare che i download del file illecito sono avvenuti a causa dei suggerimenti della piattaforma[150]. Se invece si ritenga che già la mera messa online costituisca violazione, allora l'attività organizzativo-indicizzatoria-propositiva della piattaforma non gioca alcun ruolo causale.

Infine c'è un'altra ragione che milita a favore dell'inclusione nell'area del safe harbour delle piattaforme lato sensu intese. Anche se per ipotesi si togliessero tutti i suggerimenti pubblicitari, non si avrebbero comunque risultati "puri" (o "naturali, come si dice ad es. per quelli prodotti dai motori di ricerca per contrapporli a quelli "sponsorizzati"). Parlare di risultati puri o naturali presupporrebbe che esistessero in rerum natura e cioè in via oggettiva, a prescindere dal contributo della piattaforma: il che non è[151]. Il newsfeed di Facebook e l'elenco risultati dei motori di ricerca sono totalmente frutto di un algoritmo, che, da un lato, viene costantemente modificato

[149] Si tratta però di profilo diverso, come detto sopra. Un conto è il diritto di fruire o meno del safe harbour; ben diverso conto (almeno in teoria) è se esiste o meno violazione di diritti altrui nella modalità (aquiliana o contrattuale)

[150] Conf. Nicholas J. T., *Freebooting on Facebook -- Should the Social Media Giant Face Liability?*, 25 *J. Intell. Prop. L.* 315 (2018), leggibile in https://digitalcommons.law.uga.edu/jipl/vol25/iss2/8), pp. 325-328: la non conoscenza (né effettiva né presuntiva: *actual v. constructive knowledge*) da parte di Facebook dell'illiceità dei files ospitati porta a rigettare tanto la tesi della sua responsabilità, quanto quella della perdita di safe harbour ex § 512 DMCA (il saggio esamina la pratica c.d del *freeboting*).

[151] Esprime un'idea simile Cian M., *Online Platforms as Gatekeepers to the Digital World – A Preliminary Issue on Business Freedom, Competition and the Need for a Special Market Regulation*-, *Journal of European consumer and market law*, 2018, 210: <<*Even if search neutrality is a broadly known principle, it is not suitable for ensuring a uniform access to information and equal conditions for uploaded digital contents to reach internet users: any submission of search results requires the previous choice of sorting criteria, which can be objective, while they are never neutral. For instance, displaying the most clicked webpage, the most popular video clip, or the best-rated hotel as the top-ranked result is one of many possible options; it is not the neutral one.*>> (p.210).

(spesso dopo appositi test[152]) sulla base di varie esigenze (non ultime le pressioni dirette o indirette degli inserzionisti[153]), e, dall'altro, dipende dallo stesso utente in base alla sua personale storia (tracking) di navigazione (nella misura in cui l'algoritmo lo prevede), sicchè la presentazione delle informazioni cercate varia da utente ad utente[154]. Ad es. il News Feed di Facebook non è solamente <<*a weighted formula with thousands of inputs, but rather a constantly updated, personalized machine learning model, which changes and updates its outputs based on your behavior, the behavior of people you are connected with, and the behavior of the affinity and personality-based sub-group of users the system judges you to belong to. Facebook's formula, to the extent that it actually exists, changes every day*>>[155].

[152] Bilic P., *Search algorithms, hidden labour and information control*, in *Big data § society*, January-June 2020, pp. 2-3; Baillargeon J., *Search Engine Optimization: What We See and Why We See It*, 4 *Georgetown Law Technology Review*, 2019, 303; A. Vespignani con R. Rijtano, *L'algoritmo e l'oracolo. Come la scienza predice il futuro e ci aiuta a cambiarlo*, Il Saggiatore, 2019, 114-115; Perel M. and Elkin-Koren N., *Accountability in algorithmic copyright enforcement*, 19 Stan. Tech. L. Rev., 2016, 518-519; Sumpter D., *Outnumbered: From Facebook and Google to Fake News and Filter-bubbles – The Algorithms That Control Our Lives*, Ed.: Bloomsbury Sigma, 2018, 138-139, non visto, cit. da Thompson K.A., *Commercial Clicks: Advertising Algorithms as Commercial Speech*, cit., 1030 nota 65. Quanto ai test, si tratta ad es. degli ormai noti A/B test (Quintarelli S., *Capitalismo immaterialei*, cit., p. 54/5)

[153] Sander B., *Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation*, 43 *Fordham Int'l L.J.* 939 (2020), p. 954; Keller D., *Internet Platforms: Observations on Speech, Danger, and Money*, in Hoover Institution-Aegis series paper n. 1807, 2018, p.4.

[154] Thai J., *Facebook's Speech Code and Policies: How They Suppress Speech and Distort Democratic Deliberation*, in *American University Law Review*, 2020, p. 1679-1680. Pertanto è altamente probabile che utenti diversi ottengano risposte diverse alla medesima domanda. Il dato è risaputo e v.- Susser D.-Roessler B.-Nissenbaum H., *Online Manipulation: Hidden Influences in a Digital World*, cit., 32; - Thompson K.A., *Commercial Clicks: Advertising Algorithms as Commercial Speech*, cit., 1028; Pasquale F., *The black box society*, cit., 78; v. poi l'esperimento condotto da Agosti C.-Coluccini R.-Corona G.-Romano S.-*Amazon Tracking Exposed* (dovrebbe essere del 2019). Andrebbe però approfondita l'affermazione qui presente <<non reputiamo Amazon direttamente responsabile di questa pratica, casomai lo è il venditore.>>.

[155] DeVito M.A., *From Editors to Algorithms*, in *Digital Journalism*, vol. 5/6, 753-773, a p. 768. V. poi i generali criteri di azione dei progettisti degli algoritmi (p. 756/7) e specifcicamente quelli algoritmici propri del News Feed di Facebook, in base ai documenti ufficiali reperibili. Questi ultimi sarebbero i seguenti nove, in ordine di importanza: <<*friend relationships, explicitly*

Sicchè l'idea persistente "*that platforms are open, impartial, and unregulated is an odd one, considering that everything on a platform is designed and orchestrated*"[156]. Per non dire che nei casi delicati ci sono pure interventi manuali sui risultati dei motori di ricerca[157] e che ci sono varie tecniche per ingannare il motore di ricerca, i cui esiti a loro volta contribuiranno a determinare i futuri page rankings[158]. Quindi non ci sono offerte naturali od oggettive di risultati: tutto è solo frutto delle istruzioni algoritmiche, sottoposte a continuo cambiamento. Il punto è stato ben colto in una nota sentenza statunitense *Search King c. Google Technology* del 2003: <<*However, this reasoning ignores the important distinction between process and result. Here, the process, which involves the application of the PageRank algorithm, is objective in nature. In contrast, the result, which is the PageRank — or the numerical representation of relative significance of a particular web site — is fundamentally subjective in nature. This is so because every algorithm employed by every search engine is different, and will*

expressed user interests, prior user engagement, implicitly expressed user preferences, post age, platform priorities, page relationships, negatively expressed preferences, and content quality>> (ivi, p. 766).

[156] Gillespie T., *Custodians of the internet*, cit., 21/2. V. ivi anche il cap. 2 *the myth of the neutral platform*, p. 24 ss. Si tratta di dato comune: Gerbaudo P., *I partiti digitali. L'organizzazione politica nell'era delle piattaforme*, cit., p. 97/8 (ricordando altro saggio di Gillespie); in questo interessante saggio l'a. rileva non poche somiglianze organizzative tra i partiti politici attuali e le piattaforme digitali (ad es. **p**. 99 ss).

[157] Cosa alquanto prevedibile ed anzi quasi ovvia. E' comunque emersa ad es. dalle interessanti audizioni dei CEOs delle quattro Big Tech di fine luglio 2020 sui profili antitrust (<<*Online Platforms and Market Power-Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google*>>, v. in particolare quello a Sundar Pichai di Google-Alphabet) da parte della Commissione Giustizia della House of Representatives, che hanno dedicato attenzioni notevoli alle denunce di manipolazione dei risultati delle ricerche in base ai più vari interessi delle piattaforme. Sintesi delle condotte emerse dalle audizioni in Singer H., *Top 10 Admissions from Tech CEOs Secured at the Antitrust Hearing*, promarket.org, 31.07.2020.

[158] Tecniche dette *black hat SEO (search engine optimization):* Baillargeon J., *Search Engine Optimization*, cit., 302 e 305. V. Pasquale F., *The black box society*, cit., 64/5. Ad ogni modo gli stessi Larry Page e Sergey Brin ammisero a suo tempo di aspettarsi che <<*advertising funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers*>> (riportato in Pasquale F., *The black box society*, cit., 71) e in tale senso v. Katyal S., *Private accountability in the age of artificial intelligence*, 66 *UCLA law review* 54 (2019), p. 70..

produce a different representation of the relative significance of a particular web site depending on the various factors, and the weight of the factors, used to determine whether a web site corresponds to a search query>>[159].

La "passività" di questi internet provider non esiste né è mai esistita, sicchè il mito della loro c.d. "neutralità", è appunto solo un mito[160]. Ne segue che, se si insiste nel pretenderla, le piattaforme attuali, anche in ipotesi optassero per rimuovere ogni pubblicità, per il solo fatto di prestare il servizio informativo in base ad algoritmo da loro creato, non potrebbero

[159] Search King, Inc. v. Google Technology, Inc., Case No. CIV-02-1457-M, 6 (W.D. Okla. May. 27, 2003), p. 3-4. Tuttavia la distinzione tra algoritmo e risultati, per dire che solo il primo è *objective in nature*, è assai discutibile, visto che, da un lato, i secondi dipendono in toto dal primo, il quale, dall'altro, a sua volta opera attuando le istruzioni in esso inserite dai programmatori. La sentenza nega ogni responsabilità di Google per aver arretrato nell'elenco risultati (Search Engine Results Page, SERP) il sito dell'attore (fatti sub 1.1), dato che il Page Rank è espressione di diritto di parola: <<*PageRanks are opinions-opinions of the significance of particular web sites as they correspond to a search query. (…) The Court simply finds there is no conceivable way to prove that the relative significance assigned to a given web site is false. Accordingly, the Court concludes that Google's PageRanks are entitled to "full constitutional protection*>>, p. 4). Similmente U.S. District Court, M.D. Florida, Fort Myers Division, *e-ventures Worldwide, LLC v. Google, Inc*, 188 F. Supp. 3d 1265 (M.D. Fla. 2016) del 12 maggio 2016, caso n° 2:14-cv-646-FtM-29CM: <<*The Court finds these cases persuasive that Google's PageRanks are pure opinions of the website's relevancy to a user's search query, incapable of being proven true or false*>>, (sub *B. First Amendment Defense*) e poi, tra le stesse parti, U.S. District Court Middle District Of Florida, e-Ventures Worldwide v. Google, 08.02.2017, caso n° 2:14-cv-646-FtM-PAM-CM: <<*A search engine is akin to a publisher, whose judgments about what to publish and what not to publish are absolutely protected by the First Amendment. (…) The presumption that editorial judgments, no matter the motive, are protected expression is too high a bar for e-Ventures to overcome*>>, p. 8. Non solo non esiste alcuna neutralità delle piattforme dato che, <<*per via dell'l'imperativo dell'estrazione e della neessità di un'economai di scala, i capitalisti della sorveglianza devono attrarre una marea infinita di contenuti sulle proprie spiaggie: non si limitano ad ospitare contenuti, ma se ne servono per estrarre valore in modo aggressivo, segreto e unilaterale*>> (Zuboff S., *Il capitalismo della sorveglianzai*, cit., 122-123).

[160] Douek E., *Governing Online Speech: From 'Posts-As-Trumps' to Proportionality and Probability* (August 23, 2020), in *Columbia Law Review*, Vol. 121, No. 1, 2021 Forthcoming, letto in ssrn.com, pp. 16-18.Si v. J. E. Cohen, *Tailoring Election Regulation: The Platform is the Frame*, in *Georgetown law technology review*, vol. 4/2, 2020, p. 655, nonché le otto ragioni per cui la neutralità non esiste, esposte da Chander A.-Krishnamurthy V., *The Myth of Platform Neutrality*, July 2018, in *Georgetown Law Technology review*, p. 403 ss., e le ragioni per cui Silicon valley l'afferma (ivi, sub II, 410-413).

mai fruire del safe harbour. Non credo che questa sia la scelta ordinamentale: il fatto, che non esistessero all'epoca della dir. 2000/31, non impedisce di interpretarla in via evolutiva, per tener conto di come si sono modificati da allora i servizi internet di questo tipo.

9. Ancora ipotizzando di applicare il cons. 42 all'hosting provider

Inoltre, sempre ipotizzando di applicare il cons. 42 al tipo hosting provider, servirebbe pure un adattamento del cons. medesimo. Il suo primo periodo (<<le deroghe alla responsabilità stabilita nella presente direttiva riguardano esclusivamente il caso in cui … più efficiente la trasmissione>>), infatti, come sopra accennato, è applicabile solo ai primi due tipi di provider, non alla memorizzazione duratura. Rimarrebbe testualmente applicabile la seconda parte, che è così condensabile: i) attività meramente tecnica, automatica e passiva; di conseguenza ii) il prestatore non conosce le informazioni memorizzate; e iii) nemmeno le controlla.

I punti ii) e iii) sono soddisfatti. Infatti non si può dire che egli conosca i contenuti dell'enorme numero di file presenti sui suoi server. Nemmeno si può dire che li controlli, dato che sono caricati e gestiti dai suoi utenti. E' vero che immancabilmente nei contratti con costoro il provider/piattaforma si riserva il diritto di modificare, elaborare, riprodurre, etc. i materiali: ma si tratta di potere che di fatto, a quanto immagino, non viene esercitato se non in remote eventuali ipotesi, tra cui: evitare azioni di inadempimento o risarcimento del danno nel caso provveda a rimuovere i contenuti e/o disabilitare l'accesso perché richiesto dal soggetto leso o ingiunto dal giudice e/o violazione della policy della piattaforma.. Invece il controllo, che fa perdere il safe harbour, è quello che viene usualmente esercitato nei fatti, in modo che si possa dire che anche il provider ha contribuito alla diffusione in rete: ad es. quando filtrasse in modo volutamente lasco i file manualmente o anche informaticamente, opportunamente settando i parametri per permettere il passaggio di certi temi o siti. Ma si tratterebbe di prova difficile per il soggetto leso e che comunque, per restare in tema, venendo offerta ex post, non potrebbe escludere ex ante dal safe harbour le piattaforme, che procedono ai consueti

trattamenti di elencazione, organizzazione, indicizzazione etc.[161]. A proposito del profilo del controllo, può ricordarsi la differenza tra il modello di business di Spotify e quello di Youtube: il primo sceglie e controlla totalmente e in piena autonomia i contenuti che propone, sicchè sa esattamente quali sono in un dato momento (in sostanza è una responsabilità c.d. editoriale); Youtube si limita a organizzare i contenuti caricati dagli utenti[162].

Profilo interessante, perché la riserva di eseguire la censura sui contenuti (o la sua applicazione reale, per chi ne chiede l'effettività, come a me pare), da un lato, tutela contrattualmente il provider verso il suo cliente; dall'altra, però, rischia di fargli perdere il safe harbour per la ragione appena accennata e cioè perché può dirsi che egli abbia il controllo sull'operato del cliente stesso (art. 14 § 2 dir art. 16 c. 2 d. lgs. 70/2003). C'è quindi da valutare per un provider, se convenga realmente filtrare i contenuti: se non lo fa, mantiene il safe harbour perché è neutro e quindi la sua responsabilità sorge solo quando ha notizia del singolo illecito, secondo la disciplina dell'art. 16 d. lgs. 70/2003; se invece filtra, rischia di perdere il safe harbour, anche se probabilmente si salverà comunque, in quanto la sua condotta sarà ritenuta diligente e quindi non colposa ex art. 2043.

Anche il punto sub i) (attività meramente tecnica, automatica e passiva), tutto sommato, può dirsi rispettato, come sopra anticipato. E' probabile che il legislatore UE non avesse in mente questo tipo di attività: negli anni 1999-2000 (sarebbe da

[161] Ritiene invece che la predisposizione di clausole, che riservano al provider ampi poteri, in sostenza gli attribuisca il controllo dei contenuti Trib. MI 09.09.2011 cit. nel processo *RTI c. Yahoo* cit. p. 747.

[162] La differenza di modello di business è valorizzata da Bridy A., *The Price of Closing the "Value Gap"*, cit., 327. L'a. spiega come la potente spinta dell'industria musicale sia all'origine dell'art. 17 dir. 2019/790 di modifica del copyright europeo: voleva infatti chiudere il preteso *value gap* tra profitto delle piattaforme e profitto proprio (eccessivamente ridotto, a suo dire), allo scopo parificando i due modelli di business (Spotify e Youtube) per cercare di percepire anche dal secondo quello che riesce a percepire dal primo. Vi si è aggiunta pure la spinta prodotta da uno dei due produttori mondiali di filtri automatici (automated content recognition: ACR), la soc. Audible Magic (l'altro è Google con Content-ID), che ha visto nell'imposizione di una loro obbligatoria adozione una straordinaria occasione di business (Bridy A., *The Price of Closing the "Value Gap"*, cit, 341, segnalando l'assenza di concorrenza nel relativo mercato: ivi, 350).

verificare) ancora non esistevano le predette caratteristiche del servizio di hosting. In ogni caso, leggendo bene il cons. 42, la conseguenza del rispettare tale punto i) è quella, di cui alla prosecuzione del cons. ("il che implica che non conosce né controlla" i contenuti), che abbiamo appena visto venir rispettata. In altre parole, i profili della tecnicità, automaticità e passività, sono menzionati in relazione all'unico effetto, che per il cons 42 pare rilevante: che ne consegua l'assenza in capo al provider della conoscenza o del controllo delle informazioni (cioè dei contenuti). Dovremmo allora concludere che il punto sub i) è rispettato pure dalle attuali modalità di conduzione delle piattaforme di hosting. In fondo tutti sanno che sui contenuti esse non incidono e che l'unico loro intervento è nell'ampliare e facilitare le possibilità di ricerca e individuazione delle informazioni, cui si è interessati (per generare maggior esposizione alla pubblicità, naturalmente). Questo può portare forse a facilitare (statisticamente) le violazioni[163], ma non ne è affatto conseguenza necessaria e comunque non è verificabile in relazione allo specifico caso sub iudice.

E allora, riprendendo le osservazioni anticipate sopra, la domanda è se questo aspetto collida col concetto di attività meramente i) tecnica, ii) automatica e iii) passiva. Circa i) la risposta dovrebbe essere negativa, dato che, per come si è sviluppato il mercato, questi suggerimenti indicizzati sono per lo più quelli desiderati dai navigatori e dunque fanno parte necessaria del servizio. Tecnicamente, è offerto e desiderato così dall'utente: cioè è quest'ultimo che in base al tracciamento dei suoi dati inseriti nell'algoritmo determina l'offerta o i suggerimenti. Circa ii) la risposta è pure negativa, dato che essi son attuati tramite complessi software. Circa iii) la difficoltà è apparentemente maggiore, dato che di fatto il provider non si astiene affatto, ma propone nuovi contenuti simili. Però l'interpretazione corretta del requisito ha a che far col contenuto (come conferma il riferimento del seguente cons. 43 all'alterazione della integrità della informazione)[164] e si è visto

[163] Sarebbe da verificare se l'aumento dell'offerta tramite proposte automatiche (di video su Youtube, di post su facebook, di risultati naturali o sponsorizzati su google etc.) aumenti in modo più o meno che proporzionale i download di files con materiale illecito.

[164] Sanna P., *Il regime di responsabilità dei providers intermediari di servizi della società dell'informazione,* in *Resp. civ. prev.*, 2004, 287/8 e 290, scrive a

che su di essi il provider ben raramente si intromette; per cui si può dire che contenutisticamente il provider non svolge affatto un ruolo attivo. In conclusione, le consuete modalità propositive dei contenuti, praticate dalle piattaforme, paiono rimanere all'interno delle attività ammesse dal cons. 42.

Nessun rilievo sotto questo profilo possiede la circostanza, per cui il provider percepisce un compenso dalle proposte commerciali connesse ai contenuti da lui organizzati e proposti ai navigatori. La disciplina, infatti, concede il safe harbour a chi non sa dei contenuti o a chi, appena sa dell'illiceità, li rimuove; con questo la maggior o minor lucratività non ha alcun ruolo[165].

Potrebbe ravvisarvi forse un ostacolo alla tesi qui sostenuta nell'art. 14 c. 1 lett. b)-c), d. lgs. 70/2003, laddove esclude il safe harbour per l'access/mere conduit provider che selezioni i destinatari o le informazioni. Se, anziché dare accesso o trasmettere tutto ciò che gli viene richiesto, egli filtra in modo da far passar alcune cose si ed altre no oppure in modo da permettere l'invio a Tizio ma non a Caio, è sensato che non goda di un ombrello protettivo a priori. Potrà ex post non essere ritenuto concorrente (nell'illecito costituto da ciò che ha lasciato passare), ma appunto ex post, non esentatone ex ante.

Ci si potrebbe infatti chiedere se questa ragione fosse da applicare pure all'hosting provider, per poi escludere l'ombrello protettivo nel caso dell'indicizzazione/organizzazione/promozione de qua. La risposta dovrebbe essere negativa, sia perché la disposizione specifica tace sul punto, sia perché l'hosting provider propone file/post ulteriori (in base alla sua "storia") rispetto a quelli visionati, senza modificare alcun programma di invio o trasmissione di un ipotetico soggetto inviante: "selezionare", invece, significa filtrare e cioè ridurre il numero dei contenuti/post inviati o dei destinatari di un ipotetico atto

questo proposito di necessità di un <<contatto qualificato con l'informazione veicolata>>.

[165] Punto sostanzialmente pacifico: per tutti v. C.G. 23.03.2010, *Google France v. L. Vuitton e altri*, proc. riuniti da C-236/08 a 238/08, § 116; App. MI 09.09.2011 cit. p. 747 che però, come visto, conclude diversamente considerando linsieme delle mdoalitò di offerta di Yahoo. Negli USA c'è una disposizione ad hoc: § 512 (c)(1)(B) DMCA: <*[if the service provider] does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity*>.

trasmissivo a monte. L'intervento del provider, dunque, è sostanzialmente di tipo opposto nei due casi (l'attività promozionale delle piattaforme determina un ampliamento oggettivo o soggettivo di ciò che gli utenti chiedono; l'altro determina una riduzione selettiva): per cui la regola, posta per l'uno, non può essere estesa all'altro. Questa osservazione vale non solo per il profilo oggettivo (contenuti id est, "informazioni" ex art. 14 cit.), ma anche per il profilo soggettivo (selezione dei destinatario).

10. Alcune sentenze sul punto della pretesa necessità che si tratti di provider passivi

Sul punto, come comprensibile, si è pronunciata diversa giurisprudenza, europea e nazionale. Quanto alla prima, ricordo Google France v. Vuitton e altri in tema di marchi circa il servizio pubblicitario "di posizionamento" AdWords, in cui -in base al quantum pagato- l'inserzionista si pone più in alto o più in basso nei risultati delle ricerche. Qui la Corte si limita a dire che anche per l'hosting provider si applica la regola del cons. 42[166] e che per l'accertamento della passività è semmai rilevante non il servizio in sé di posizionamento, ma <<il ruolo svolto dalla Google nella redazione del messaggio commerciale che accompagna il link pubblicitario o nella determinazione o selezione di tali parole chiave>>, ciò che tocca al giudice nazionale verificare (§ 118-119). Alla fine però esclude che il suo ruolo sia attivo (§ 120).

Più significativo è il dictum nel caso L'Oreal ed altri c. eBay ed altri ove la Corte dice che <<*Come ha giustamente osservato il governo del Regno Unito, la mera circostanza che il gestore di un mercato online memorizzi sul proprio server le offerte in vendita, stabilisca le modalità del suo servizio, sia ricompensato per quest'ultimo e fornisca informazioni d'ordine generale ai propri clienti non può avere l'effetto di privarlo delle deroghe in materia di responsabilità previste dalla direttiva 2000/31 (v., per analogia, sentenza Google France e Google, cit. punto 116).*

[166] Limitandosi a parafrasarlo: <<al fine di verificare se la responsabilità del prestatore del servizio di posizionamento possa essere limitata ai sensi dell'art. 14 della direttiva 2000/31, occorre esaminare se il ruolo svolto da detto prestatore sia neutro, in quanto il suo comportamento è meramente tecnico, automatico e passivo, comportante una mancanza di conoscenza o di controllo dei dati che esso memorizza>>, § 114.

Laddove, per contro, detto gestore abbia prestato un'assistenza consistente segnatamente nell'ottimizzare la presentazione delle offerte in vendita di cui trattasi e nel promuovere tali offerte, si deve considerare che egli non ha occupato una posizione neutra tra il cliente venditore considerato e i potenziali acquirenti, ma che ha svolto un ruolo attivo atto a conferirgli una conoscenza o un controllo dei dati relativi a dette offerte. In tal caso non può avvalersi, riguardo a tali dati, della deroga in materia di responsabilità di cui all'art. 14 della direttiva 2000/31>> (§§ 115-116)[167]: con l'immancabile aggiunta per cui l'accertamento, se ciò ricorra nel caso specifico, spetta al giudice nazionale rinviante (§ 117). Dunque secondo la C.G. l'ottimizzare la presentazione delle offerte in vendita e la loro promozione gli fa perdere il ruolo passivo e osta all'invocabilità del safe harbour. La posizione è nel metodo immotivata, dato che queste attività non costituiscono conoscenza né controllo dei contenuti (ciò che per la Corte conferisce il ruolo attivo: § 113), e nell'esito non condivisibile. Tale presa di posizione è stata seguita da sue successive pronunce[168].

In analogo senso alcuni giudici italiani come Trib. Roma RTI c. Vimeo n. 693/2019 del 10.01.2019 RG n.23732/2012 (ed altri

[167] Passaggio ripreso più sinteticamente e quindi tralaticiamente (senza appoggio motivatorio) da C.G. 11.09.2014, C-291/13, *Sotiris Papasavvas c. 3*, §§ 43-44 e da C.G. 07.08.2018, C-521/17, *SNB-REACT c. Deepak Mehta*, § 48. Nel primo caso un soggetto aveva agito verso l'editore ed alcuni giornalisti per articoli a suo dire diffamanti, pubblicati su un quotidiano cartaceo e sui relativi siti internet. Nel secondo caso il provider forniva un un servizio di locazione e registrazione di indirizzi IP, che consentiva ai suoi clienti di utilizzare anonimamente nomi di dominio e siti Internet: spetta allora al giudiice del rinvio verificare <<*che un simile prestatore non conosca né controlli le informazioni trasmesse o memorizzate dai suoi clienti e che non svolga un ruolo attivo consentendo a questi ultimi di ottimizzare la loro attività di vendita online*>> (§§ 42 e 49-50). Lo dà per scontato en passant l'AG Campos Sánchez-Bordona nelle Conclusioni 28.11.2019, C-567/18, *Coty Germany GmbH c. Amazon*, con una fugace citazione delle sentenze L'Oreal e Google France (§ 63).

[168] Ad es. da C.G. 07.08.2018, *SNB-REACT c. Deepak Mehta*, C-521/17, § §47-48, che in presenza di un servizio di locazione e registrazione di indirizzi IP conclude -immancabilmente e sbrigativamente- osservando "*in tali condizioni, spetta al giudice del rinvio, alla luce dell'insieme degli elementi di fatto e di prova pertinenti, verificare che un simile prestatore non conosca né controlli le informazioni trasmesse o memorizzate dai suoi clienti e che non svolga un ruolo attivo consentendo a questi ultimi di ottimizzare la loro attività di vendita online*>;

ivi citati)[169] e come due successive decisioni di Trib. Roma con uguale relatore (ma diverso dalla prima[170]), aventi sempre RTI come attore e Dailymotion da un lato e Vimeo dall'altro come convenuti[171].

Prendiamo queste ultime due e in particolare la prima di esse (RTI c. Dailymotion), dato che il ragionamento è sostanzialmente uguale per la parte di interesse. Il Tribunale in generale accoglie la distinzione tra hosting provider attivo e

[169] P. 15 in generale e pp. 17-18 applicato al caso specifcio (con scarna motivazione). Vimeo è un portale di video. Vedi successivamente Trib. Roma 02.10.2019 n. 18727/2019, RG 33915/2017, *RTI c. Bit Kitchen Inc.* (piattaforma *Vid.me*), p. 7, il quale però dalla perdita del diritto al safe harbour fa conseguire automaricametne la conoscenza in capo al provider della illiceità dei file ospitati: <<*Non è neppure necessario soffermarsi in questa sede sulla completezza della diffida ovvero sulla idoneità di essa a consentire la compiuta individuazione da parte del destinatario dei video da rimuovere, dato che, nel caso di specie, per quanto sopra detto, l'attività del prestatore è da qualificare come di hosting attivo, sicché deve ritenersi la conoscenza dell'illiceità dei contenuti da parte del gestore del Portale prescindendo dalla comunicazione di essa da parte del danneggiato*>> (p. 8). La tesi è errata: graverebbe la piattaforma di responsabilità oggettiva o presunta senza argomentarne il fondamento: servirebbe invero norma espressa (mancante) o un'applicazione analogica delle norme esistenti (implausibile). Secondo questo Tribunale, poi, la natura attiva della piattaforma *Vid.me* è deducibile dal fatto che, a fronte dell'allegazione di RTI che la sua attività consisteva nell'organizzare, promuovere, catalogare i file messi on line e permetterne la ricerca, sarebbe stato onere di Bit Kitchen <<*documentare che lo svolgimento di tali attività si fosse eventualmente reso possibile anche senza l'effettiva conoscenza dei contenuti illeciti diffusi tramite il portale*>> (ivi): ciò che non ha fatto, essendo restata contumace. L'affermazione lascia perplessi, dato che: 1) contrasta con la giurisprudenza europea (G. 12 luglio 2011, L'Oreal e altri c. eBay, C-324/09) per la quale l'ottimizzazione condotta da eBay della presentazione delle offerte dei clienti non le dà conoscenza dei contenuti (§ 123); affermazione quest'ultima, per altro, discutibile dato che manipolare le offerte commerciali è cosa diversa dalla conoscenza dei contenuti di cui al cons. 42 dir. 2000/31, essendo automatica; per cui la loro messa in sequenza causale nel cons. 42 dir. 2000/31 è oggi incerta e va vagliata nel singolo caso (per non dire che il cons. 42 non è applicabile all'hosting provider, come altrove spiegato in questo saggio). Il giudice avrebbe quindi eventualmente dovuto accertare il funziomanento di tali ottimizzazioni commerciali e vedere se integravano la conoscenza ex cons. 42; 2) crea la presumzione pretoria per cui tali attività sempre comportano la conoscenza dei contenuti illeciti (presunzione però priva di base giuridica) oppure applica un onere di contestazione circa detti fatti cognitivi ad una parte contumace, in violazione dell'art. 115 cpc Ci sarebbe poi la generale questione dell'onere della prova delle circostanze richieste per il safe harbour: ricade sull'attore o sul provider (solitamente) convenuto?

[170] Forse c'è un orientamento dichiaratamente condiviso dalla sezione XVII.

[171] Trib. Roma del 12.07.2019, n. 14757, *RTI c. Dailymotion*, RG 24711/2012 e Trib. Roma del 12.07.2019, n. 62343, *RTI c. Vimeo*, RG 62343/2015.

passivo, per escludere il primo dal safe harbour. Quest'ultimo presuppone il "*solo stoccaggio dei dati in maniera tecnica automatica e passiva senza e conoscenza e controllo dei dati memorizzati*", per cui perde la neutralità <<*allorquando in relazione a determinati contenuti audiovisuali e sulla base delle emergenze processuali emerga che abbia perso il carattere di neutralità e passività alla base di tale esenzione, operando sui dati che carica forme di intervento volte a sfruttare i contenuti dei singoli materiali caricati dagli utenti e memorizzati sui propri server ed operando in generale sotto le forme del controllo, della conoscenza e della profilazione dei dati ed in maniera non automatizzata*>>[172]. Nello specifico applicando tali principi, ritiene Dailymotion hosting provider attivo, dato che <<*si tratta quindi di un'archiviazione forse automatica (anche se il consulente tecnico d'ufficio ha parlato di uno staff a ciò dedicato e risultano dal bilancio costi per il personale superiore a 3,5 milioni di euro nel 2017, circostanza questa che lascia supporre l'esistenza di un nutrito gruppo di soggetti impiegati stabilmente nelle attività collegate alla gestione della piattaforma) ma sicuramente non "neutra" nel senso inteso dalla direttiva ed interpretato dalle Corti, perché finalizzata ad una gestione dei dati ad esclusivo profitto della società convenuta che presuppone un vaglio dei contenuti memorizzati (…). L'archiviazione, almeno per quanto concerne i contenuti video oggetto del presente procedimento, secondo degli specifici indici che collegano ad una de-terminata categoria potenziali e maggiori introiti pubblicitari, sono serio indice di coinvolgimento della società nella gestione dei contenuti.(…) In altre parole DAILYMOTION, lungi dall'operare quale semplice intermediario, ovvero per amore della libertà di espressione e per la divulgazione del pensiero, sembra perseguire la veicolazione e la diffusione più ampia possibile di filmati a mezzo internet massimizzando le visualizzazioni, poiché da ogni video divulgato trae i suoi utili per la vendita di servizi pubblicitari collegati alla diffusione dei filmati. La calibrazione e la profilazione pur effettuate ex ante, forse anche solo a mezzo di cookies, non escludono un disegno preventivo finalizzato alla gestione/manipolazione complessiva del materiale caricato. È difatti sempre l'uomo, secondo degli schemi ben precisi, che*

[172] p. 15-16.

profila i cookie di profilazione>>[173]. Come osservato sopra, il principale motivo alla base di questo giudizio (il profitto tratto dalle proposte di video ai navigatori) è a mio parere ininfluente sulla applicabilità del safe harbour previsto per l'hosting provider[174].

In senso opposto (e preferibile) altre pronuncia secondo cui "*il punto di discrimine tra fornitore neutrale e fornitore non neutrale debba esser individuato nella manipolazione o trasformazione delle informazioni dei contenuti trasmessi o memorizzati come peraltro suggerito (sebbene con riferimento alle attività di "mere conduit" e "caching") dal considerando n. 43 della Direttiva 2000/31/CE, estensibile, per analogia, anche al caso dell'hosting, nonché come anche chiarito dai successivi considerando n. 44 e 46 che richiamano l'intenzionalità e l'inerzia di fronte a specifiche informazioni dell'avvenuto illecito quali momenti di discrimine per il venir meno dell'operatività delle deroghe di responsabilità*." per poi precisare che <<*se invero il fornitore di servizi internet, non si limita a un mero ruolo di intermediario fra due soggetti distanti mettendo a disposizione la propria piattaforma tecnologica, ma rielabora o partecipa alla redazione del contenuto intermediato, si avrà in questo caso una piena responsabilità civile secondo le regole comuni. Qualora invece vengano attuate delle mere operazioni volte alla migliore fruibilità della piattaforma e dei contenuti in essa versati (attraverso - ad esempio - il caso tipico della indicizzazione o dei suggerimenti di ricerca individualizzati per prodotti simili o sequenziali ovvero quello altrettanto tipico dell'inserzione pubblicitaria e*

[173] Trib. Roma del 12.07.2019, n. 14757, *RTI c. Dailymotion*, RG 24711/2012, cit., p. 22-23. Gli scopi della profilazione sono stati così classificati: i) infer or predict information; ii) score, rank, evaluate and assess people, iii) make or inform a decision about an individual, iv) make or inform a decision that personalises an individual's environment (Kaltheuner F.-Bietti E., *Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR*, in *Journal of Information Rights, Policy and Practice*, 2018, 2(2), § 2.2, ove interessanti considerazioni sulla profilazione).

[174] Critico sulla tesi, che ritiene il profitto ostativo al safe harbour, è anche Wang J., *Regulating hosting ISP's responsabilities for coyright infringement*, cit., 62-64. Per questo a. l'unico criterio per decidere se riconoscere o meno il safe harbour è accertare se il provider, nel gestire i file, ne conosce i contenuti o se li controlla: per cui va negato quando si è avvantaggiato del contenuto illecito, del quale però avesse previa conoscenza (p. 69),.

dell'abbinamento di messaggi pubblicitari mirati), le predette clausole di deroga di responsabilità continueranno ad operare poiché nel caso in esame ci si troverà nell'ambito di espedienti tecnologici volti al miglior sfruttamento economico della piattaforma, e non già innanzi a un'ingerenza sulla creazione e redazione del contenuto intermediato>>[175]. La conseguenza è che tutta l'attività pubblicitaria e di indicizzazione di Youtube non gli fa perdere la neutralità[176]. Analoga è la posizione espressa l'anno seguente sempre dal Tribunale torinese tra le stesse parti in un diverso sviluppo processuale della lite[177].

Nella stesa linea si colloca il cit. appello Milano 2015 nella lite RTI c. Yahoo[178]. Secondo questo giudice <<*le attuali tecnologie avanzate, in mancanza di altri elementi in grado di fare intravedere una vera e propria manipolazione dei dati immessi da parte dell'hosting provider, non siano da sole in grado di determinare il mutamento della natura del servizio di hosting provider di tipo passivo (secondo la classificazione utilizzata dalla giurisprudenza nazionale richiamata dalla sentenza appellata), in servizio di hosting provider di tipo attivo, in ragione della mera presenza i) di sofisticate tecniche di intercettazione del contenuto dei file caricati, attraverso un motore di ricerca, e ii) delle più svariate modalità di gestione del sito e iii) del particolare interesse del gestore a conseguire vantaggi economici*>> (§ 24) dato che "*il regime di esonero dalla responsabilità, espressamente previsto nell'art. 14 della direttiva, non viene certamente intaccato dalla presenza di indici di attività meccanica e non manipolativa nel trattamento dei dati immessi, come è stato meglio specificato nel caso C-324/09, L'Oreal c. eBay*>> (§ 27).

[175] Trib. Torino sent. 1928 del 07.04.2017, RG 38112/2013, *Delta TV c Google – Youtube*, sub 6.2 p. 22/3 che subito ritiene applciabile detta regola abnche all'hosting provider.

[176] Trib. Torino sent. 1928 del 07.04.2017, cit.,k p.26-27. Il Tribunale sembra però confondere la fruizione del safe harbour con la violazione del diritto azionato (nel caso: diritto d'autore) laddove dice <<*viceversa, un intervento che valorizzi quel video - inserendolo in un indice, abbinandovi della pubblicità pertinente alla sua tipologia, oppure rendendolo visibile accanto a video similari – non comporta il venir meno della neutralità, poiché non incide affatto sul contenuto del video (e, nel caso in esame, dell'opera tutelabile ex legge n. 633/1941).*>> (p. 27)

[177] Trib. Torino n. 342 del 24.01.2018 RG 5135/2015, *Dailymotion c. Delta ITV Broadcasting c. TVCatchup*, p. 19

[178] App. Milano 07.01.2015 n. 29, RG 3821/2012, *Yahoo c. RTI*.

Il giudizio è avallato dalla seguente decisione di legittimità, la cit. Cass. 7708/2019, che ritiene corretta l'affermazione di fruibilità dell'ombrello protettivo ex art. 16 d. lgs. 70/2003 da parte della sezione Video del portale Yahoo[179]. Tuttavia la S.C., pur giungendo a tale esito nel caso specifico, ritiene errata la negazione a priori di rilevanza giuridica all'hosting provider attivo[180]: anzi, tale nozione "può ormai ritenersi dunque un approdo acquisito in ambito comunitario" (sub § 4.2). Tra l'altro cita a conforto un considerando di una versione antecedente della attuale dir. 790/2019 sulla modifica del diritto d'autore[181]: il passaggio è però errato. Da un lato, ciò potrebbe intendersi nel senso opposto e cioè nel senso che la precisazione del cons. serve proprio perché la normativa ex dir. 2000/31 non dava rilevanza all'hosting provider attivo. Dall'altro, i considerando non hanno forza normativa autonoma, per cui cedono ad un testo incompatibile con esso: ed è proprio il caso de quo, dato che il seguente art. 13 non menzionava tale pur importantissima regola, la quale quindi non poteva ritenersi posta dall'art. 13 medesimo, muto sul punto, e di conseguenza doveva ritenersi abbandonata. In ogni caso il problema è superato dal testo finale della dir. (successivo al deposito di Cass. 7708/2019) ed anzi pare modificato in direzione opposta: scomparsa l'affermazione del precedente cons. 38, l'attuale cons. 61, 3° e 4° periodo, dice che la ratio di introduzione della nuova disciplina (che qualifica d'imperio l'hosting di materiali coperti da diritto d'autore come comunicazione al pubblico) consiste nel superare l'incertezza

[179] § 4.4 di Cass. 7708/2019 che ne corregge la motivazione ex art. 384 n. 4 cpc

[180] § 38 della cit. App. Milano 07.01.2015 n. 29, RG 3821/2012, *Yahoo c. RTI*.

[181] la S.C. cita il cons. 38 della Proposta di DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO sul diritto d'autore nel mercato unico digitale COM/2016/0593 final - 2016/0280 (COD). i cui primi due periodi (tralascio l'ultimo periodo, irrilevante) così dicevano "*Qualora i prestatori di servizi della società dell'informazione memorizzino e diano pubblico accesso a opere o altro materiale protetti dal diritto d'autore caricati dagli utenti, andando così oltre la mera fornitura di attrezzature fisiche ed effettuando in tal modo un atto di comunicazione al pubblico, essi sono obbligati a concludere accordi di licenza con i titolari dei diritti, a meno che non rientrino nell'esenzione di responsabilità di cui all'articolo 14 della direttiva 2000/31/CE del Parlamento europeo e del Consiglio 34. Per quanto concerne l'articolo 14 è necessario verificare se il prestatore di servizi svolge un ruolo attivo, anche ottimizzando la presentazione delle opere o altro materiale caricati o promuovendoli, indipendentemente dalla natura del mezzo utilizzato a tal fine*.>>

giuridica della condotta di chi ospita materiali protetti. Tale affermazione di incertezza giuridica, allora, contraddice la giurisprudenza europea citata. Inoltre, passando all'articolato, il fatto, che l'articolato sia ancora una volta muto sul punto in esame, non permette di ravvisare nella dir. 790 alcun elemento a favore della perdita del safe harbour nel hosting provider c.d. attivo[182].

Nella stessa linea da me sostenuta pare Cass. pen. III, ud. 17.12.2013 e dep. 03.02.2014 n. 5107 (caso *Google c. Vividown*), che trova conforto in tale posizione per negare a Google/Youtube la titolarità del trattamento dati personali, riservandola solo agli utenti uploader (§§ 7.2-8).

Così anche la giurisprudenza statunitense sulle piattaforme di videosharing, che ha riconosciuto loro il safe harbour di cui al § 512(c) del 17 US code, molto simile a quello europeo[183]. Si consideri quanto osserva il giudice in *Viacom v. Youtube <<As previously noted, the District Court held that the statutory phrases "actual knowledge that the material... is infringing" and "facts or circumstances from which infringing activity is apparent" refer to "knowledge of specific and identifiable infringements." [...] For the reasons that follow, we substantially affirm that holding*.>> (§ 39) e poi circa le funzioni di *transcoding* e di *play-back* a vantaggio dell'utente: *<<The relevant case law makes clear that the § 512(c) safe harbor extends to software functions performed "for the purpose of*

[182] La dir. 2019/790 infatti non menziona minimamente i requisiti di indicizzazione/organizzazione/promozione posti dalla C.G. L?Oreal e oggi dalla nostra Cassazione 7708/2019, che –forse un po' precipitosamente- si è spinta addirittura ad elencare dei c.d. indici di inteferenza: "*Dunque, si può parlare di hosting provider attivo, sottratto al regime privilegiato, quando sia ravvisabile una condotta di azione, nel senso ora richiamato. Gli elementi idonei a delineare la figura o "indici di interferenza", da accertare in concreto ad opera del giudice del merito, sono - a titolo esemplificativo e non necessariamente tutte compresenti - le attività di filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione dei contenuti, operate mediante una gestione imprenditoriale del servizio, come pure l'adozione di una tecnica di valutazione comportamentale degli utenti per aumentarne la fidelizzazione: condotte che abbiano, in sostanza, l'effetto di completare ed arricchire in modo non passivo la fruizione dei contenuti da parte di utenti indeterminati*".

[183] V. sentenze *Capital Records LLC c. Vimeo* del 2016, *UMG Recordings Inc. c. Shelter Capital Partners* del 2013 e *Viacom c. Youtube* del 2012, citt. da Bridy A., *The Price of Closing the "Value Gap"*, cit., 334-335, testo e note 49-50.

facilitating access to user-stored material." [...] Two of the software functions challenged here—transcoding and playback—were expressly considered by our sister Circuit in Shelter Capital, which held that liability arising from these functions occurred "by reason of the storage at the direction of a user." [...] Transcoding involves "[m]aking copies of a video in a different encoding scheme" in order to render the video "viewable over the Internet to most users." [...] The playback process involves "deliver[ing] copies of YouTube videos to a user's browser cache" in response to a user request. [...] The District Court correctly found that to exclude these automated functions from the safe harbor would eviscerate the protection afforded to service providers by § 512(c)>> (§ 77) (grassetto aggiunto)[184].

11. Sintesi del ragionamento sul tema della pretesa passività

In sintesi, che grandi provider spingano al massimo per la fruizione di quanto caricato dagli utenti, è indubbio, dato che i relativi contenuti permettono spazi pubblicitari e la rilevazione di dati con cui affinare gli algoritmi; che questo sia incompatibile col disposto del cons. 42, invece, è assai dubbio. In particolare, circa il secondo periodo di tale cons., non pare eccedere l'"attività meramente tecnica e passiva" essendo stata creata apposta per sfruttare in automatico e in via massiva i dati degli utenti[185]. Nemmeno però è interpretabile come conoscenza

[184] *Viacom International v. Youtube*, 676 F.3d 19, United States Court of Appeals, Second Circuit, Decided: April 5, 2012, leggibile in cyber.harvard.edu. La corte distrettuale infatti aveva così esattamente posto i termini della questione: <<*Thus, the critical question is whether the statutory phrases "actual knowledge that the material or an activity using the material on the system or network is infringing," and "facts or circumstances from which infringing activity is apparent" in § 512(c)(1)(A)(i) and (ii) mean a general awareness that there are infringements (here, claimed to be widespread and common), or rather mean actual or constructive knowledge of specific and identifiable infringements of individual items*>> (U.S. District Court-Southern district of N.Y., 23 giugno 2010, giudice Stanton, caso 07 Civ. 2103 LLS; grassetto aggiunto). La decisione è stata poi confermata da United States District Court-Southern district of New York, 18 aprile 2013, giudice Stanton.

[185] Zuboff S., *Il capitalismo della sorveglianza*, cit., passim: l'a. fa notare che è questo il motivo per cui i provider non sono solleciti nell'esaudire la richeista iniziale del soggetto leso. Lo strapotere dei FAGA (Facebook, Amazon, google, Apple; l'acronimo può variare, leggendosi pure FANG, Facebook, Amazon, Netflix, Google; o FAANG, Facebook, Amazon, Apple, Google, Netflix), al punto che alcuno li chiama i *data barons* (evocando i *robber barons* statunitensi del

1800: v. Zuboff S., *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri,* LUISS Univ. Press, 2019 (orig.: 2019), 116-117; Mayer-Schönberger-K. Cukier, *Big data*, Garzanti, 2013, non visto, cit. da Mezza M., *Algoritmi di libertà*, Donzelli, 2018, 193), dato sia dalla loro concentrazione che dalla necessità quasi assoluta –reale o creduta, è irrilevante- per i più di avvalersene, induce a pensare che poco cambierà pur dopo: i) la necessità di consenso al trattamento, spt. ex art. 6, art. 9 e art. 22 § 1-2-3 per la profilazione, GDPR; ii) l'eccezione di text and data mining della dir. 790/2019 per il diritto d'autore (art. 3, per scopi di ricerca scientifica, e art. 4, per ogni scopo e ammesso per default, tranne un implausibile opt-out espresso in modalità appropriata e cioè che consenta la lettura automatizzata per le opere pubblicmetne disponibili on line); § 3); iii) l'eventuale consolidazione dell'orientamento favorevole alla nullità di alcune clausole contrattuali proposte/imposte dalle grandi piattaforme, sancito per ora da tre note pronuncice francesi tra il 2018 e il 2019, quanto al diritto del consumatore. Pare più speranzosa invece S. Scalzini, *L'estrazione di dati e di testi per finalità commerciali dai contenuti degli utenti. Algoritmi, proprietà intellettuale e autonomia negoziale*, Anal. giur. econ., 2019/1, 395 ss, §§ 4-5 (con riferimento ai punti ii)-iii)). Intanto la normativa è deficitaria ed anche quella europea, pur dopo l'avanzamento dato dal GDPR: è condivisibile l'affermazione per cui il consenso non è libero (art. 4 n. 11, GDPR) se risponde ad un offerta standardizzata e da fonte monopolistica, e il trattameotn non è corretto (art. 5 § 1 sub a, GDPR) se discrimina tra soggetti o preclude l'accesso a beni fondamentali (G. Resta, *Governare l'innovazione tecnologica: dcisioni algoritmiche, diritti digitali e principio di ugualianza*, in *An. giur. econ.*, 2019/1, 205-6). Tuttavia accanto a buone innovazioni, la disciplina presenta pure carenze, laddove ad es. per la profilazione il divieto ex art. 22 GDPR: i) concerne solo la decisione totalmentte automatizzata, ii) deve trattarsi di una "decisione", iii) deve essere produttiva di "effetti giuridici" sull'utente oppure "incidere in modo analogo significativamente sulla sua persona": per cui non comprende la pubblicità e in particolare il microtargeting (conf. G. Resta, *Governare l'innovazione tecnologica*, cit., 225/6), a meno di non pensare al successivo ricevimento di offerte commerciali, le quali -come offerte al pubblico *in incertam personam*, se non anche individualizzate- producono l'effetto della soggezione dell'offerente alla conclusione del contratto ex art. 1336 cc o della proposta ordinaria); iv) è oscuro il meccanismo applicativo del divieto ex art. 22 § 1, restando incerto se il controdiritto dell'interessato sia strutturato –potremmo dire- come opt-in (spetta all'interessto attivarsi, altrimenti il trattamento è lecito) oppure come opt-out (il divieto opera pienamente fin da subito, salvo consenso dell'interessato) ed è probabilmente esatta la seconda alternativa (conff.: Kaltheuner F.-Bietti E., *Data is power*, cit., 10-11; Brkan M., *Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond*, in *International Journal of Law and Information Technology*, Volume 27/2, 2019, p. 99 ss., https://doi.org/10.1093/ijlit/eay017, con analitica e convincente argomentazione; Kaminski M.E., *The Right to Explanation, Explained*, 34 Berkeley Tech. L.J. 189 (2019), 201 leggibile in https://scholar.law.colorado.edu/articles/1227.; Castets-Renard C., *Accountability of Algorithms in the GDPR and Beyond: A European Legal Framework on Automated Decision-Making*, 30 Fordham Intell. Prop. Media & Ent. L.J. 91 (2019), 112; Noto La Diega G., *Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information*, 2018, JIPITEC, 3 ss., §

47), valendo anche per gli atti dispositivi della privacy quanto vale per la sottoposizione a trattamenti sanitari e cioè che il consenso libero e informato non può mai essere presunto o tacito (Cass. 10.12.2019 n. 32.214; anche la privacy è infatti un diritto fondamentale, come risulta dall'art. 7 Carta dei diritti fondamentali dell'UE, c.d Carta di Nizza, e dalle sentenze sul diritto all'oblio C.G. 13.05.2014, *Google Spain c. AEPD-Gonzalez*, passim -ad es. §§ 74, 80 87, 97- e C.G. 24.09.2019, *Google c. Wikimedia e altri*, C-507/17, § 45, pur se meno importante del diritto alla salute), non parendo confliggere con discipline europee (interessante sarebbe ragionare sulla legittimità di un'ipotetica regola opposta, cioè dell'opt-in); v) in ogni caso, già l'averne consepevolezza è problematico, visto che l'accesso per verificare la sottoposizione a trattamenti automatizzati e a profllatura (art. 15 § 1 lett. h GDPR) è di incerta discplina, dato che secondo il cons. 63 GDPR da un lato non dovrebbe violare diritto di autore (ogni software ne è protetto! anche se si può dire che non lo violerebbe) e, dall'altro, però, ciò "non dovrebbe[-ro] condurre a un diniego a fornire all'interessato tutte le informazioni" (ma il cons. non ha forza normativa per cui non può dire ciò che l'articolato non dice), vi) la *human review* ex art. 22/3 GDPR difficilmente si discosterà dall'esito algoritmico per due difetti cognitivi, consistenti nella tendenza anche inconsapevole a considerarlo superiore e migliore di quello umano e nella difficoltà di ignorare le informazioni una volta che sono state comunicate, al pari di quanto avviene per le istruzioni probatorie negative impartite ai giurati nel processo statunitense (Geslevich Packin N., *Consumer Finance and AI: The Death of Second Opinions?*, 22 *N.Y.U. J. Legis. & Pub. Pol'y 319* (2020), a 366-368; invero dipenderà da come sarà strutturato il processo di revisione, per cui le perplessità potrebbero essere altre, come ad es. l'influenza dei *desiderata* ufficiali o informali del management aziendale); vi) l'assenza di tutela, quando la decisione sia necessaria per concludere o eseguire un contratto (art. 22 § 2 lett. a)), sposta il problema a monte, dato che la disposizione resta muta sul concetto di <necessità>, essendoci il rischio che l'interessato dichiari che ricorre detta necessità in modo automatico e/o senza reale libertà (simile preoccupazione in Falletti E., *Deciisoni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche, Dir. informazione informatica*, 2020/2, 179). Il problema reale è l'enorme disparità di forza contrattuale che la lascerà per lo più inapplicata: a fronte di qualche sporadico caso, lo sfruttamento dei dati proseguirà sistematicamente e incessantemente, tranne l'esperimento di vigorose azioni collettive (similmnte G. Resta, *Governare l'innovazione tecnologica*, cit., 226/7 e 235/6): a proposito di un confronto tra l'allora venticinquenne Zuckerberg e il ministro tedesco per la Consumer Protection Ilse Aigner, l'Economist nel 2010 notava che <<*"it is hard to say who is the David," and who the Goliath*>> (leggo in A. Chander, *Facebookistan, North Carolina Law Review*, vol. 1807, 2012, 1819, nelle cui pagg. segg. trovi un resoconto delle relazioni di Facebook con alcuni Stati e nelle cui pagg. precedenti un esame del se Facebook possa definirsi Stato o Nazione). Per non dire che la tutela ex art. 22 GDPR riguarda solo le decisioni "totalmente" automatizzate e quindi non quelle in cui ci sia un qualunque intervento umano, anche minimo: potendosi o dovendosi però correggere il dettato letterale, nel senso che l'intervento umano, escludente la tutela, sia solo quello in cui sono esercitate funzioni cognitive e/o volitive, in grado di influire sulla decisione, e non solo materiali o puramente esecutive (così pure vari aa. tra cui: Brkan M., *Do algorithms rule the world?*, cit., 101; Castets-Renard C., *Accountability of Algorithms in the GDPR and Beyondi*, cit., 111/2; Sesso Sarti O., *Art. 22 Reg. 2016/679 GDPR*, in *Comm. cod. civ.* dir. da Gabrielli, *Delle*

o controllo dei contenuti. La situazione dunque è dubbia, ma al momento è preferibile permettere anche a questo tipo di business il safe harbour, sulla base di i) un argomento letterale e ii) di uno teleologico. Quanto ad i), l'art. 14 –certamente prevalente sui cons.- e l'art. 16 d. lgs. 70/2003 non menzionano i requisiti di cui al cons. 42. Quanto ad ii), viene rispettata la ragione del safe harbour[186], consistente nel non applicarsi a condotte imprenditoriali che facilitino consapevolmente le violazioni: eventualità che non ricorre, dato che come sopra ricordato, le promozioni commerciali si rivolgono indistintamente a tutti i contenuti, senza distinguere tra fonti lecite e illecite. Perciò non può dirsi che l'attività di indicizzazione/organizzazione/promozione favorisca

Persone-Leggi Collegate, II, a cura di Barba-Pagliantini, Utet giuridica, 2019, 479; Article 29 Data Protection Working Party (WP29), *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 03.10.2017-06.02.2018, IV.A, p. 20-21). Simili osservazioni in Simoncini A., *Profili costituzionali della amministrazione algoritmica*, in *Riv. dir. pubbl*., 2019, 1172-1174 (che segnala la maggior ampiezza della tutela interna – almeno per come emerge dalla giurisprudenza amministrativa ivi esaminata- rispetto a quella europea: v. pure p.1175 ss). Al potere dei citt. FAGA, in Cina corrisponde quello dei BAT (Baidu, Albaba, Tencent), mentre analoghe iniziative (politico-)imprenditoriali non son riuscite in Europa, pur se questa fa da battistrada nella regolazione, soprattutto col GDPR: così Daly A., *Neo-Liberal Business-As-Usual or Post-Surveillance Capitalism With European Characteristics? The EU's General Data Protection Regulation in a Multi-Polar Internet*, 19 July 2020, letto in ssrn.com, pp. 8-10 e 13 (l'a. è critica sulla reale protezione offerta dal GDPR, che faciliterebbe troppo il commercio di dati personali, pp. 13-16, passim)..

[186] Desumibile da un esame sistematico della disciplina (soprattutto dal caching provider: art. 15 lett. e e al diveito di soerveglianza generale) e dalla considerazione della soggerzione ad inibitorie anche se il provider nulla sa dell'illecito: ma da quel momento, se non ottempera, concorre. Si v. l'AG 22.09.2009, C da 236/08 a 238/08 nel caso *Google France*: <<*A mio parere, lo scopo della direttiva 2000/31 consiste nel creare un dominio pubblico aperto e gratuito su Internet. Essa persegue tale scopo limitando la responsabilità di coloro che trasmettono o memorizzano informazioni, ai sensi degli artt. 12-14 della medesima direttiva, ai casi un cui tali soggetti fossero a conoscenza di attività illecite. Per il conseguimento di tale scopo è decisivo l'art. 15 della direttiva 2000/31, che vieta agli Stati membri di imporre ai prestatori di servizi dell'informazione un obbligo di sorveglianza sulle informazioni che trasmettono o memorizzano, o di verificarne attivamente la liceità. Ritengo che l'art. 15 di detta direttiva non si limiti ad imporre un obbligo negativo agli Stati membri, ma sia l'espressione stessa del principio secondo cui i prestatori di servizi che intendano beneficiare di un'esenzione di responsabilità devono rimanere neutri rispetto alle informazioni che trasmettono o memorizzano*.>> (§§ 142-143)

(consapevolmente) le seconde: questa in fondo è la ragione del safe harbour, anche nella versione immaginata dal cons. 42, come risulta dalla proposizione finale "il che implica che il prestatore di servizi della società dell'informazione non conosce né controlla le informazioni trasmesse o memorizzate". Valutazione che potrà essere riconsiderata, anche alla luce di maggiori informazioni sugli algoritmi che governano il funzionamento delle piattaforme.

E' vero che questo sistema serve a promuovere non solo merci ma –questo è l'aspetto più preoccupante- pure idee, dal lato utente, e vendite o impieghi di dati personali, dal lato inserzionista[187]. Già sono stati evidenziati i seri e gravi pericoli per i processi politico/democratici e sociali in genere, derivanti dalla qualità di gatekeepers globali della comunicazione[188], alla

[187] La pubblicità on line ha un'insaziabile fame di dati dei consumatori, per cui Google e Facebook <<*increasingly ignore user privacy, they collect an ever-growing amount of data from their users' emails, search queries, browsers, social network likes, and online video consumption, to target consumers and dominate online advertising*>>. Il duopolio costituito da queste due piattaforme raccoglie il 60 % di tutto l'internet advertising statunitense, come pure la larga maggioranza dei suoi incrementi annuali (così D. Srinivasan, *The Intersection of Privacy, Data, and Competition*, in promarkert.org, 26.10.2019, 2); Google da sola ha il 37% del digital advertising mondiale e il 78 % del search advertising statunitense (H. Singer, *Monopolization in the Name of Privacy: Google Is Slowly But Steadily Closing Its Advertising Ecosystem*, in promarket.org: l'a. descrive le manovre di Google per impedire la tracciabilità da parte di terzi degli utenti del proprio browser Chrome, ad es. impedendo la rilevazione dei dati relativi ai DNS -domain naming system- ma non solo). <<*Rather, their business model requires them to induce as many people as possible around the world to post, speak, and broadcast to each other. Constant production of content by end-users, in turn, captures audience attention. This allows digital media companies to sell advertising, collect data about end-users, and use this information to sell even more advertising. The twentieth century model required large audiences*>> (J.M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, UC Davis Law Review vol. 51, 3, febrary 2018, 1192).

[188] *Gatekeepers* sono i "*non-state actors with the capacity to alter the behaviour of others in circumstances where the state has limited capacity to do the same*" (Hörnle J., *Gatekeepers on the Internet: The Role of Intermediaries in Local Enforcement* (December 9, 2019), p. 2, riportando le parole di altro a.). Il termine viene spesso usato per le piattaforme: ex multis v. ad es. Bell E., *The unintentional press*, cit., passim, ad es. 237, 242 e 247/8). Nel contesto del giornalismo il gatekeeping si riferisce <<*to the process by which news organizations make decisions as to which of the events taking place or issues being discussed received coverage*>> (Napoli P., *Social media and the public interest*, cit., 54). Al giorno d'oggi il ruolo di *gatekeeping* algoritmico va contro ciò che molti si aspettavano dal primo Internet e cioè contro l'idea di internet come

luce dell'esponenziale incremento dei dati passanti sui loro server[189], soprattutto dopo l'incremento di comunicazione digitale a seguito della pandemia del 2020[190] (anche se si

disintermediator (Napoli P., ivi, 58 ss ove esame del mutamento radicale del sistema di produzione e distribuzione di notizie e, p. 66 ss, dell'incidenza sui media informativi tradizionali come in generale tutto il cap. 2 *Algorithmic gatekeeping and the transformation of news organizations*): "*l'apparente disintermediazione politica [che] è invece –assai più subdolamente- "neointermediazione" ad opera dei soggetti che vedono crescere il proprio valore societario sui mercati finanziari grazie alla cattura e gestione dei dati*" (Valastro A., *Internet e social media prima e dopo il coronavirus: fraintendimenti e deviazioni che tradiscono la democrazia sociale*, in *Liber Amicorum per Pasquale Costanzo*, giurcost.org, 20.04.2020, p. 10) e conformi Barberis M., *Populismo digitale. Come internet sta uccidendo la democrazia*, ChiareLettere, 2020, 37-39 e 44-45 (v. p. 156 segg. i motivi per cui l'*homo mediaticus/digitalis* è alla base dei populismi attuali) e Gerbaudo P., *I partiti digitali*, cit., p. 95/6 (<*se le compagnie digitali eliminano gl interemediari preesistenti, al contempo esse creano nuove forme di intermediazione a un livello più alto*>). Si leggono però altri significati attribuiti al concetto di *gatekeeper*, come ad es. quello di *property ownners that may permit and restrict access to their websites much like landowners may do with private land in the real word* (Kadri T., *Digital gatekeepers*, in *Texas law review*, 2021, forthcoming, p. 4 e 9-11, ove resoconto di ulteriori significati): l'a. riferisce dunque la propria definizione alla necessità di consenso per estrarre dati dai siti web, pur aperti indistamente al pubblico, a seguito del Computer fraud and abuse act-CFAA- del 1986, evidenziandone i rischi per la concorrenza (p. 16 ss.) e proponendo rimedi de iure condendo (p. 29 ss).

[189] Circa la content moderation, v. Langvardt K., *Regulating Online Content Moderation*, in *Georgetown law journal*, vol. 106, 2018, p. 1358 ss, che spiega la differenza della *content moderation* attuale rispetto al governo dei flussi informativi dell'epoca analogica (o anche rispetto a quello dei primi tempi di internet) e scrive di *moderators'dilemma* (tra il desiderio/dovere di filtrare i contenuti inappropriati e il rischio di censura preventiva).

[190] V.si Waters R.-McGee P.-Murphy H., *Big Tech defies global economic fallout with blockbuster earnings - Apple, Amazon, Facebook and Google prosper in face of virus pandemic and regulatory scrutiny*, Financial Times, ed. on line, 31.07.2020 (con paywall). V. poi il breve ma chiaro e preciso saggio di Cobbe J.-Bietti E., *Rethinking Digital Platforms for the Post-COVID-19 Era*, 21.05.2020, cigionline.org. Addirittura la *content moderation* lederebbe il principio costituzionale della separazione dei poteri secondo Perel M.-Elkin-Koren N., Guarding the Guardians: Content Moderation by Online Intermediaries and the Rule of Law (February 23, 2020), ssrn.com, 669-670 e 672, in quanto sarebbero al tempo stesso legislatori, giudici e agenzie amministrative (decidendo sul filtraggio preventivo o successivo). L'affermazione è eccessiva a livello teorico, in quanto –da noi almeno- i diritti fondametnali, posti o riconosciuti dall'ordinamento statale, sempre prevalgono su eventualmente contrarie regole interne dei social e in quanto l'azione in corte è sempre ammessa. Però non va lontano dal vero a livello fattuale: quanti sono i soggetti lesi dalla censura dei social o discriminati dall'advertising mirato ad agire in giudizio contro questi colossi?

dimenticano altre pressioni sul gioco democratico, assai meno visibili[191], e anche se taluno riesce a cogliere ciò nonostante un fenomeno di *balkanization* dell'internet, con ritorno a walled gardens[192]). Tali pericoli sono legati soprattutto:

-alla riduzione del tasso di esposizione ad idee diverse dalle proprie (filter bubbles ed echo chambers[193], le seconde diverse

[191] Come ad es. quelle esercitate dai maggiori investitori finanziari mondiali (fondi di investimento, banche d'affari, etc.; oppure quelle dipendenti dalla sorveglianza esercitata dai governi con o senza le big tech (i cui reciproci rapporti restano totalmente oscuri), su cui v. ad es.: - Giglioli M.F.N., *I labirinti della sorveglianza informatica*, Il Mulino, 2019, passim ma spt. capp. I-II (di taglio sociologico); - Lubin A., *The liberty to spy*, *Harvard International Law Journal*, vol. 61/1, 2020, p. 185 ss e spt. I e II, p. 211 ss sullo *jus ad explorationem*, per cui a gli Stati "*enjoy a peacetime right to spyunder international law, that the existence of the right is essential for thefunctioning of our public world order, and that only by acknowledging theright may we be able to articulate when the right is abused*", p. 189; - Lyon D., *La cultura della sorveglianza*, cit., passim, ad es. 131ss o 143 ss. (ma il tema costituisce un altro *Leitmotiv* del libro, valorizzando le rivelazioni di Edward Snowden); - l'autobiografia di Edward Snowden, *Errore di sistema*, Longanesi, 2019 (orig.: 2019), cap. 13 segg.

[192] Lemley M.A., *The Splinternet*, (July 30, 2020), in *Stanford Law and Economics Olin Working Paper*, Forthcoming, letto in ssrn.com. con riferimento ai muri (normativi) elevati dai governi: non solo in Cina, Russia ed India ma anche altrove, tra cui in Unione Europea, di cui l'a. coglie la differenza d'approccio rispetto agli USA (p.5/6)

[193] Il testo di riferimento è l'eccellente lavoro di Sunstein C., *#Republic.com*, cit., tutto, ma soprattutto i capp. I-VI. Si v. anche Ainis M., *Il regno dell'uroboro. Benvenuti nel'era della solitudine di massa*, La nave di Teseo, 2018, passim (ad es. 17, 43, 64, 93 e 109), con particolare accento sull'isolamento sociale che ne segue, e Thuy Vo L., *How the Internet created multiple publics*, in Georgetown Law Technology Review, vol. 4/2, p. 399 ss (2020). Ne segue il rischio di immobilismo sociale ed anzi di crescente polarizzazione delle opinioni verso gli estremi (Ro'ee Levy, *Social Media, News Consumption and Polarization: Evidence from a Field Experiment*, 08.11.2019, Yale University, spt. §§ 5 e 8; Diamond J., *Crisi. Come rinascono le nazioni*, Einaudi, 2019 (orig.: 2019), 308/9, che lo ricollega pure alla tv via cavo, assai diffusa negli Stati Uniti; Thuy Vo L., *How the Internet Created Multiple Publics*, in *Georgetown law technology review*, vol. 4/2, 2020, 399 ss, passim, per cui il social web è il posto in cui <nuance goes to die>, p. 409; Banerjee A.V.-Duflo E., *Una buona economia per tempi difficili*, Laterza, 2020 (orig. 2019), p. 149 ss e 157 ss., verosimilmente riposante sullla –evolutivamente- naturale e comprensibile tendenza ad associarsi ai propri simili, c.d *omofilia*); per non dire del rischio di usare una *predictive justice* che perpetui –quasi profezia autoavverantesi- pregiudizi e cliché etcnico-sociali nella valutazione di pericolosità effettuata nei giudizi penali (L. Eckhouse, *Big data may be reinforcing racial bias in the criminal justice system*, washingtonpost.com, 10.02.2017; K. Rahnama, *Science and Ethics of Algorithms in the Courtroom*, *University of Illinois-Journal of Law, Technology & Policy*, 2019, no. 1, Spring 2019, 169-18, inammissibile da noi secondo Soro A., *Democrazia e potere dei dati*, cit., 169-173, passim, 180 circa il divieto di

profilazione ex art. 8 d. lgs. 51 del 2018, 186), amplificata dal fatto che pacchetti di dati e di decisioni algoritmiche vengono poi venduti ad altre imprese (J.M. Balkin, *Free Speech in the Algorithmic Society*, cit., 1167-8; Wilka R.-Landy R.-McKinney S.A., *How Machines Learn: Where Do Companies Get Data for Machine Learning and What Licenses Do They Need?*, 13 *Wash. J. L. Tech. & Arts 217* (2018), passim (sub IV, p. 231 ss per le fonti di acquisizione dei dati necessari al machine learning) o anche trattati come merce di scambio in più ampie operazioni societarie, magari "per aiutare amici": O. Solon-C. Farivar, *Leaked documents show Facebook leveraged user data to fight rivals and help friends*, nbcnews.com, 06.11.2019) o vengono incrementati a seguito di concentrazioni giustificate proprio dal pacchetto di nuovi dati che così si conseguono (F. Yun Chee-V.Waldersee, *After Google's Fitbit deal, EU says worrying when firms targeted for their data*, uk.reuters.com, 07.11.2019, circa l'acquisto di Fitbit – produttrice di dispositivi elettronici indossabili per il fitness- da parte di google: è noto che questi dispositivi sono quelli che Zuboff indica come propri del prossimo passo evolutivo della sorveglianza da parte delle Big Tech e non a caso Facebook aveva cercato prima di Google ma senza successo di acquisire Fitbit, come si legge in rete) o ceduti a Google da Ascension, seconda impresa di assistenza sanitaria degli Stati Uniti, nel Project Nightingale e senza consenso dei pazienti, pur se qui pare esserci una certa copertura normativa (notizia diffusa da R. Copeland, *Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans*, Wall Street Journal, 11.11.2019 –ove il video che spiega l'interesse delle Big Tech per i dati sanitari- e subito ripresa da altri ad es. da E. Pilkington, *Google's secret cache of medical data includes names and full details of millions – whistleblower*, guardian.co.uk, 12.11.2019. Il mercato dei dati sanitari deve essere assai interessante, essendo fiorente pure in Europa (v. l'indagine del Financial Times sul Regno Unito in M. Murgia-M. Harlow, *How top health websites are sharing sensitive data with advertisers*, www.ft.com, 13.11.2019, e v. pure il saggio Angelica N., *Alexa's artificial intelligence paves the way for big tech's entrance into the health care industry – the benefits to efficiency and support of the patient-centric system outweigh the impact on privacy*, *North Carolina J. of law & tech*., vol. 21/4, 2020, 59 ss, ove resoconto dei profili di data protection –con giudizio sostanzilamente positivo- dell'uso dell'AI nella gestione dei dati sanitari e dell'accordo tra Amazon e Cerner, una delle due maggiorni compagnie statunitensi di electonic health record), per non menzionare ora l'eventualità che raccolgano pure i dati finanziario-reddituali (T. Bradshow, *Google in talks to move into banking Move follows Apple's credit card launch and Facebook's proposed Libra currency*, www.ft.com, 13.11.2019). Sull'interesse dei governi per i dati raccolti dalle piattaforme e sul conseguente sfumare della distinzione pubblico e privato (State and Market) v. Pasquale F., *The black box society*, cit., 48 ss., 156 ss., 206 ss. (sul rischio di "cattura del regolatore da parte del regolato") e 215. Rischio di immobilismo sociale, dicevo, che vale pure per il processo civile, come ad es. nel risalente caso della stima del danno da lucro cessante in relazione alla vita futura professionale di un ragazzo leso, proveniente da famiglia non abbiente. C'è già qualche caso. Si v. l'ormai celeberrimo caso *State of Wisconsin c. Loomis*, discusso di solito in ricerche sul rischio di discrminazioni, e commentato un po' dappertutto, definito da condanna a sei anni di reclusione dell'afroamericano Eric L. Loomis sulla base dell'algoritmo COMPAS (Correctional Offender Management Profiling for Alternative Sanctions: software propreitario di Northpointe, ora Equivant), per il quale egli era ad alto rischio di recidiva. Da un

lato, la Corte suprema del Wisconsin ha negato che l'inaccessibilità alla conoscenza dell'algoritmo a causa della tutela della proprietà intellettuale violasse il dirtto ad un processo equo; dall'altro, inchieste giornalistiche (Propublica) hanno fatto sorgere il dubbio che Compas avesse pregiudizi verso gli afroamericani, ancbhe per la sola ragione che era stato costruito con tutti i precedenti giudiziari, notoriamnte sfavorevoli alle categorie più deboli (prendo da A. Celotto, *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, *Anal. giur. econ.*, 2019, 1, 47/8). Del resto, essendo retrospettivo, non può che riflettere l'esistsente divario nei livelli di istruzione e sociali in genere (principio del GIGO – "garbage in garbage out" – per cui un algoritmo non può che riflettere la qualità dei dati su cui è costruito: A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, Rivista di BioDiritto, n. 1/2019, 85, sub 5.3; O'Donnell R.M., *Challenging Racist Predictive Policing Algorithms Under the Equal Protection Clause*, in *New York university law review*, 2019, vol. 94/3, 544 ss, al § I.C, 553 ss, addirittura gli algoritmi, fatti interagire tra loro, svilupperebbero da sé distorsioni sistematiche, come riferisce Rumiati R., *Saper decidere. Intuizione, ragione e impulsività*, Mulino, 2020, 168-169); divario che –in quanto tale- diventa meccanismo autorinforzantesi (notazione diffusa negli studi economici recenti: ad es. in M. Alacevich-A.Soci, *Breve storia della disuguaglianza*, Lateza, 2019, 130-131). L'uso di A.I. in sede giudiziaria, soprattuttto penale, è sempre più intenso, come risulta ad es. da: Liu H.-Lin C.-Chen Y., *Beyond State v Loomis: artificial intelligence, government algorithmization and accountability*, *International Journal of Law and Information Technology*, vol. 27/2, p. 125-126 e 136; Elyounes D.A., *Bail or Jail? Judicial versus Algorithmic Decision-Making in the Pretrial System*, in *Columbia Science and Technology Law Review*, 21/2, 2020, p. 376 ss., secondo cui i sette *AI risk assessment tools*, da lui esaminati partitamente (sub III.A-F, tra cui l'ormai celebre COMPAS), sono già largamente usati in sei stati e in più di cento giurisdizioni (di ogni tipo: aree popolate ma anche rurali ed isolate, p.380-381). Non c'è solo il profilo dell'accuratezza dei dati di partenza, naturalmente. La Corte Suprema del Wisconsin, ad es., avrebbe rigettato l'istanza dell'imputato focalizzandosi solo sull'accuratezza dei dati e dimenticando i criteri di loro valutazione (essenzialmente relativi alla categorizzazione delle persone e all'attribuzione del peso specifico a ciascuna fattore): questo l'errore denunciato in Washington A., *How to Argue with an Algorithm: Lessons from the COMPAS ProPublica Debate* (February 4, 2019), in *Colorado Technology Law Journal*, 2018, volume 17/1,131 ss., spt. 134 e 144-148. Anche nell'A.I. *machine-learning* ogni pregiudizio (*bias*), presente nei dati usati per il training iniziale, si riprodurrà nelle decisioni successive: il punto parrebbe anche qui ovvio ed è comunque esaminato approfonditamente da molta dottrina, tra cui: - Bathaee Y., *The artificial intelligence black box and the failure of intent and causation*, cit., p. 920; - Barocas S.-Selbst A.D., *Big Data's Disparate Impact*, 104 *California Law Review* 671 (2016), sub I, pp. 677-693, leggibile in ssrn.com; - v. poi in Elyounes D.A., *Bail or Jail?*, cit. sopra in questa nota, le interessanti tavole comparative dei sette AI tools usati nei pretrials criminali (p. 425 ss.) e in particolare quella sul *data quality assessment* e cioè sulla quantità di casi usati per sviluppare ciacun tool (che varia drasticamente da soli 452 in Ohio a 750.000 con il Public Safety Assessment (PSA) della Arnold Foundation, p. 430). Il medesimo (credo) software Compas è stato protagonsta di analoga controversia in Florida: è stato però fatto notare che esistono diverse accezione di "imparzialità" (parità predittiva; eguaglianza di falsi positivi; ed anzi altre ancora), sicchè la questione

è delicata (A. Vespignani con R. Rijtano, *L'algoritmo e l'oracolo*, cit., 106-110): e lo dimostra un interessante lavoro sul concetto di *algorithmic fairness*, il quale, ricordata l'esistenza in letteratura di oltre venti definizioni di fairness nella computer science (p. 4), propone una triplice distinzione tra fairness a livello individuale (P. 7 ss), a livello di gruppo (p. 15 ss) e a livello di nesso di causalità (o meglio a livello di nesso tra causalità e correlazioni, per scegliere la più elevata ma anche razionalmente soddisfacente delle seconde, p. 30 ss): Abu-Elyounes D., *Contextual Fairness: A Legal and Policy Analysis of Algorithmic Fairness*, in *Journal of law, technology policy*, 2020, 1 ss (v. griglie riassuntive della sua proposta a p. 7 e 37; ma la scelta dipenderà dalle circostanze, p. 6). A Chicago un "predictive policing tool" (TRAP - Targeted Repeat-Offender Apprehension Program) è stato abbandonato per le discriminazioni cui dava luogo (lo riferisce C. Doctorow su boingboing.net, 25.01.2020). Si v. poi l'algoritmo che sostituisce le cauzioni a pagamento, introdotto nel 2018 in California per evitare disparità socioeconomiche: Solow-Niederman A.-Choi Y.-Van der Broeck G., *The institutional life of algorithmic risk assessment, Berkeley Technology law journal*, 2019, vol. 34, 2019, 705 ss (per i quali questi strumenti sono sempre più diffusi a livello statale e locale, p. 714; per l'esame analitico del suo funzionamento v. parti III-IV; pende però referendum sulla legge introduttiva, promosso dagli imprenditori dei servizi finanziari connessi all'attuale cauzione monetaria, p. 708 nota 12). Il rischio di discriminazioni negli output dell'algoritmo, naturalmente, c'è per tutte le attività che se ne avvalgono, pubbliche ma anche private, come ad es. nella stipula di assicuirazioni o di finanzamenti (Battelli E., *Big data e algoritmi predittivi nel settore assicurativo: vantaggi e nuovi rischi*, Il corr. giur., 2019,. 12, 1517-1518; Gillis T.B.-Spiess J.L., *Big Data and Discrimination, The University of Chicago Law Review*, 2019, vol. 86/2, 459 ss; Katyal S., *Private accountability in the age of artificial intelligence*, cit., p. 95 sulla riduzione del fido su carta di credito basata su big data e non sul rapporto in essere; Hollreiser J.F., *Closing the Racial Gap in Financial Services: Balancing Algorithmic Opportunity with Legal Limitations*, in Cornell law review, maggio 2020, vol. 105/3-4, sub III, 1249-1255) o anche nella diffusione di offerte di lavoro (Blass J., *Algoritmic advertising discrimination*, in *Northwestern University Law Review*, 2019, vol. 114 /2, 415 ss, spt. 439 ss.; Kim P. T., *Manipulating Opportunity*, cit., sub II.A-D): l'impiego di scoring (ratings) basato su algoritmi dovrebbe essere sottoposto a concessione e audit, qualora riferito ai settori più delicati (salute, assicurazioni e rapporti di lavoro) (Citron D.K., *The Scored Society: Due Process for Automated Predictions*, in *Washington Law Review*, 2014, vol. 89/1, 21/22) e gli algoritmi sottoposti a disclosure (nel diritto USA, tra i tanti: Bloch-Wehba H., *Access to algorithms*, in *Fordham law review*, 2020, vol. 88/4, 1308/1309, riferito soprattutto ai rapporti pubblicistici; l'a. scrive di *information silos* –p. 1310- per indicare che le Corti autorizzano la comunicazione delle informazioni solo alle parti, con divieto di divulgazione esterna). Per non dire dell'orwelliano social scoring/rating, apertamente adottato in Cina (Social Credit System: SCS) per promuovere la conformazione alla legge e ai valori nazionali (in Occidente descritto come un "dystopian nightmare, a prison world of pervasive surveillance feeding soul-crushing behavior modification to promote obedience to the CCP [Chinese Communist Party] ", su cui v. ad es. Werbach K., *Panopticon Reborn China's Social Credit as Regulation for the Algorithmic Age*, 2020, letto in ssrn.com (v. spt. la sua *information architecture*, sub IV.B., p. 52 ss).

dalle prime per la presenza di una scelta più o meno volontaria dell'utente, anziché dell'algoritmo[194], a dispetto dell'importanza delle esperienze condivise per creare il c.d. capitale sociale[195]; anche se si legge di una parziale retromarcia di qualcuno[196]),

[194] Così secondo M. Monti, *Regolazione, Internet e tecnica: le implicazioni di motori di ricerca e social networks sulla libertà di informazione*, *federalismi.it*, 2017/24, 25.

[195] Sunstein C., *#Republic.com,* cit., p. 180-184.

[196] Google avrebbe ora deciso la riduzione del microtargeting politico: R. Waters, *Google and the problem with microtargeting*, *Financial Times*, 22.11.2019, in www.ft.com; N. Corasaniti-M. Rosenberg, *Campaigns Say Google Ad Policy Sidesteps Problem of Disinformation*, New York Times, www.nyt.com, 21.11.2019 (v. la dichiarazione 20.11.2019 di Google a firma S. Spencer *An update on our political ads policy*). Facebook invece al momento non pare cambiare la propria policy per seguire Google: del resto, c'è un reale problema di tutela della libertà di espressione, dato che alcuni gruppi sociali o politici di fatto hanno la possibilità di farsi notare solamente tramite le piattaforme internet e Facebook in particolare, per cui una restrizione li penalizzarebbe particolarmente così come l'informazione alternativa in regimi autoritari (vedasi: - Bloch-Wehba H., *Automation in Moderation*, cit., p. 41-42 del.pdf; - M. Isaac, *Campaigns Pressure Facebook to Stay Put on Political Ads*, New York Times, 22.11.2019, The New York Times, nytimes.com; - l'ultimo rapporto annuale di *Freedom House*, *Freedom On The Net 2019. The Crisis of Social Media*, 1 e 10-11, complessivamente incentrato sul rischio, da un lato, di disinformazione elettorale e, dall'altro, di controllo pubblico-governativo tramite internet; - Geddes K., *Meet Your New Overlords: How Digital Platforms Develop and Sustain Technofeudalism*, cit., 457/8; - M. Monti, *Regolazione, Internet e tecnica*, cit., 24-25, segnalando però il rischio delle fake news, principale problema di Facebook, p. 26/7; - Cohen J.E., *Between truth and power*, cit., 86 ss., ove però anche i noti profili di rischio della polarizzazione etc.; - Kaye D., *The global struggle to govern the internet*, cit.,p. 114-115, sulla Cambogia; Langvardt K., *Regulating Online Content Moderation*, cit., p. 1355-1356 sui Rohingya nel Myanmar) o che altri gruppi traggono importante supporto tramite i social per rimediare a nuove forme di discrminazione (Cavazza N.-Guidetti M., *Scelte alimentari Foodies, vegani, neofobici e altre storie, Il Mulino,* 2020, p. 83, circa le discrminazioni a carico dei vegani). E' dubbio se e quanto le dichiarazioni delle Big Tech in proposito siano verificabili, generando quindi seri dubbi sulla compatibilità di tale comunicazione politica con le regole democratiche. L'importanza delle piattaforme per il pluralismo politico è affermata da Trib. Roma ord. 12.12.2019, RG 59264/2019, *CasaPound c. Facebook,* p.4 e 5: tale considerazione regge la decisione cautelare di accoglimento dell'istanza di riattivazione del profilo FB, assieme al mancato accertamento *prima facie* di violazioni contrattuali di CasaPound (sminuisce invece l'essenzialità della presenza sui social Weaver R., *Social media platforms and democratic discourse*, in *Lewis§Clark law* review, 2020, vol. 23/4, 1413/1414, ravvisando una *internet's resilience*). Altro tema è quello del se nella comunicazione politica rientri la diffusione di contenuti politici sponsorizzati sui social: lo negano D'Ippolito G., *Comunicazione politica online: dal messaggio politico commercializzato alle sponsorizzazioni sui social network*, Riv. dir. media, 2020/1, medialaws.eu (per il quale anzi si tratta di comunicazione di

impresa e dunque qualificabile ex art. 41 anziché 21 Cost., passim, spt. 174 e 177/8) e Parsons G.M., *Fighting for Attention: Democracy, Free Speech, and the Marketplace of Ideas*, in *Minnesota law review*, maggio 2020, vol. 104, 2157 ss., sub III.B.3.i, pp. 2211-2226. Secondo Parsons, il tradizionale concetto di *marketplace of ideas*, solitamente attribuito al giudice Holmes nella sentenza *Abrams v. United States* del 1919 (ivi, p. 2158, nota 2; anche se per vero il termine esatto non fu da lui mai pronunciato, come osserva Blasi V., *Rights Skepticism and Majority Rule at the Birth of the Modern First Amendment*, in Bollinger L.C.-Stone G.R., *The free speech century*, cit., 19, pur se il concetto emerge nitidamente dalla sentenza, leggibile ad es in law.cornell.edu, § 58; analoga idea fu espressa da Brandeis in *Whitney v. California* del 1927, salvo il limite del *clear and present danger test*, sulla cui attualità v. Sunstein C., *Does the clear and present danger test survive cost-benefit analysis?* in Bollinger L.C.-Stone G.R., *The free speech century*, cit. 162 ss) è antiquato e va sostituito con quello, potremmo dire, di <mercato dell'attenzione (*attentional choice*)> sulla base di una *attentional-choice theory of competition* (p. 2192): <<*as a matter of First Amendment theory, attentional choices could operate as the missing market mechanism at the heart of the marketplace of ideas: the link between our decentralized de-cisions as consumers of ideas about their value and the mediat-ing function that we are expected to play in deciding what de-serves further exposure in society*>> (p. 2181). Anzi a ben vedere l'idea sottostante è antica e frequentemente ricorrente nella storia della comunicazione pubblica: v. Allotti P., *La libertà di stampa*, Il Mulino, 2020, pp. 25/6 (John Milton, Inghilterra, 1644), pp. 31/2 (*Cato's Letters* di John Trenchard e Thomas Gordon, Inghilterra, 1724), 63 (Thomnas Jefferson, presidente USA, 1801), p. 103 (parlamentari inglesi abolizionisti delle c.d. *Taxes on knowledge* e John Stuart Mill, 1855 e 1858), pp. 164-165 (Ernesto Rossi, Italia, 1958). L'economia comportamentale e i bias ivi evidenziati confermano l'esattezza di questo approccio: che il marketplace delle idee (e in particolare il *counterspeech*) funzioni anche sui social media è dunque assai dubbio (critica in Napoli P., *Social media and the public interest*, cit., 88-106, passim e poi soprattutto cap. 4 *the structure of the algoritmic marketplace of ideas*, p. 107 ss., ove analisi dei fallimenti di questo mercato) per cui l'attenzione al counterspeech va ridotta (Napoli P., *Social media and the public interest*, cit., 189-191). Che la scarsità di frequenze sia sostanzialmente venuta meno è da tutti rilevato, ma non toglie che ricorra una nuova scarsità, quella dell'attenzione (*attention scarcity*): Lorenz-Spreen P.- Lewandowsky, S.-Sunstein, C.R-Hertwig R., *How behavioural sciences can promote truth, autonomy and democratic discourse online*, *Nature Human Behavoiur* (2020), p. 1 (<<*Technology companies exploit this all-important role in pursuit of the most precious resource in the online marketplace: human attention*>>), e Magarian G.P., *Forward into the Past: Speech Intermediaries in the Television and Internet Ages*, 71 OKLA. L. REV. 237 (2018), p. 264. Per altri, abbandonata la *spectrum scarcity*, il dovere delle piattaforme di rispettare l'interesse pubblico si fonda sulla considerazione per cui le vaste aggregazioni di dati, su cui esse vivono, costituiscono oggi una risorsa pubblica collettiva fonte di responsabilità sociali (Napoli P., *Social media and the public interest*, cit., 148-150; ma il concetto non mi pare chiarissimo). In breve, l'assunto "sunlight is the best disinfectant" (sempre del giudice Brandeis) è parecchio incerto ed anzi infondato nella sua assolutezza (Phillips W., *Light Disinfects*, in *Georgetown technology law review*, 2020, 379 ss., passim (spt. 386-388 e § V), dipendendo dal contesto e in particolare dal fatto che gli interessati abbiano tutti pari capacità di adeguatamente partecipare al pubblico dibattito (il

complessivamente chiamati "acceleratori tecnologici"[197], personalizzazione che mette in crisi il concetto tradizionale del pubblico dibattito, che presupporrebbe che tutti ricevessero le stesse informazioni per fare scelte informate[198]; del resto, la tendenza a frequentare persone (considerate) simili a sé fa parte della natura umana[199], avendo probabilmente ragioni biologico-evolutive profonde; con accentuazione dunque della polarizzazione verso gli estremi delle opinioni espresse nel dibattito socio-politico[200];

- alla intermediazione tra offerenti e destinatari, concentrata in un numero ridottissimo di potentissimi soggetti privati[201], a

che non avviene nel decidere il consenso sulle richieste di uso dei dati: Obar J.A., *Sunlight alone is not a disinfectant: Consent and the futility of opening Big Data black boxes (without assistance),* in Big Data & Society, 2020/1, 1-5, ove è riportato il cit. passo di Brandeis, tratto da "What Publicity Can Do"in *Harper's Weekly* del 1913): mi pare infatti legato al tradizionale concetto del cittadino come *rational listener*, che però è sostanzialmente incompatibile col modo di funzionamento delle piattaforme digitali (conf. J. E. Cohen, *Tailoring Election Regulation: The Platform is the Frame*, cit., p. 649-653).

[197] Bracciale R.-Grisolia F., *Information Disorder: acceleratori tecnologici e dinamiche social*, Federalismi, 2020/11, 24.04.2020, *federalismi.it*, spt. § 3 (gli aa. distinguono tra acceleratori tecnologici e dinamiche sociali conseguenti, inserendo le *echo chambers* tra queste ultime, § 4)

[198] Bell E., *The unintentional press*, cit., 251; Bickert M., *Defining the boundaries of free speech on social media*, in Bollinger L.C.-Stone G.R., *The free speech century*, cit., 260/1, auspicando *global standards* invece che *country-specific standards*, anche per velocizzare l'applicazione della policy di enforcement (l'a. è un dirigente di Facebook). Personalizzazione che sarebbe iniziata il 4 dicembre 2009, allorchè Google avvertì i propri utenti che da quel momento avrebbe personalizzato il motore di ricerca (così secondo Ainis M., *Il regno dell'uroboro*, cit., 12); Cassese S., *Il buongoverno. L'età dei doveri*. Mondadori, 2020, 260 ss (circa l'uso dei social in politica, ove la tecnica del rilancio "virale" è chiamato dall'a. "tecnica dell'interesse composto").

[199] C.d. *omofilia* e v. Sunstein C.R., *#Republic.com*, cit., 12; Banerjee A.V.-Duflo E., *Una buona economia per tempi difficili*, cit., p. 123 ss sull'istinto gregario e p. 149 ss sull'omofilia (ma si veda tutto il cap. 4 *Like, desideri, bisogni*).

[200] Tendenza rilevata da moltissimi autori, da essere diventato quasi un luogo comune. Curiosamente (ma, a ben vedere, non è affatto strano) anche i c.d. *small donors* nelle campagne di fund raising statunitensi, lodate come esempio di pratica democratica, in realtà sono praticate da soggetti con opinioni collocate agli estremi ed anzi maggiormente agli estremi rispetto ad altri *individual donors* (Pildes R.H., *Participation and polarization*, in *Journal of constitutional law*, vol. 22/2, sub II.B-C, p. 364 ss)

[201] Yemini M., *The new irony of free speech*, in *The Columbia science§ technology law review*, vol. XX, 2018, 119 ss., sub III.D, p. 179 ss. Si pensi al rifiuto di Google di pagare agli editori francesi il compenso previsto dal nuovo

diritto connesso creato dall'art. 15 della nuova direttiva copyright 790/2019 e della possibile conseguente retrocessione (in che misura?) nell'elenco dei risultati di chi insisterà nella richiesta (L. Kayali, *Google refuses to pay publishers in France*, politico.eu, 25.09.2019); ora pare che si limiti ad indicare nelle *news snippet* il mero titolo, sull'assunto che non violi detto art. 15, anche se non ha evitato nell'aprile 2020 un accertamento in Francia di abuso di posizione dominante, come riferisce Trevisi C., *Una stampa libera e pluralista è essenziale per garantire un giornalismo di qualità. Il diritto d'autore e i diritti connessi tutelano il patrimonio culturale*, medialaws.eu del 29.05.2020). Stante la sua dominanza assoluta, anzi quasi totalitaria in questo servizio, e il fatto che i navigatori quasi sempre si fermano dopo i primi risultati (secondo uno studio, il 91,5 per cento degli utenti si ferma alla prima pagina, mentre solamente il 4,8 per cento va alla seconda, secondo uno studio di cui riferisce G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in *riv. dir. media*, 2018/1, 25) ciò costituirà una grave penalizzazione e -per i minori- un serio rischio di quasi-deindicizzazione dal web; "e ciò che non è visibile, nel nuovo mondo digitale, rischia di non esistere" (Calisse M.-Musella F., *Il principe digitale*, Laterza, 2019, 11; v. pure p. 21 e 27; equivale ad una sentenza di morte per i concorrenti di Google la *search results demotion* per Pasquale F., *The black box society*, cit., 166, oppure al diventare invisibili al *general public* per Van Loo R., *Federal rules of platform procedure*, di prossima pubblicazione in *University of Chicago Law review*, draft 16 maggio 2020, p. 26, riferendo l'opinione di D. C. Nunziato; equivale allo scomparire dalle Yellow Pages di qualche decennio fa per Keller D., *Internet Platforms: Observations on Speech, Danger, and Money*, cit., 27). Analogamente per il marketplace di Amazon v. Angioni M., *Amazon dietro le quinte*, cit., 183-185), una nuova forma della romana *damnatio memoriae* (così G.L. Conti, *Manifestazione del pensiero attraverso la rete e trasformazione della libertà di espressione: c'è ancora da ballare per strada?*, in *Rivista Ass. Ital. Costituz.*, rivistaaic.it, 4/2018, 14.11.2018, 209-210) e per la presenza pubblicitaria su Facebook, così importante che le mediopiccole imprese non possono permettersi di partecipare al *#StopHateForProfit boycott* organizzato dagli inserzionisti maggiori nel 2020 (Carroll D., *Why Most Advertisers Can't Afford to Boycott Facebook*, promarket.org, 08.07.2020); v. sul punto Khan L., *Sources of Tech Platform Power*, 2 *Georgetown law technology review* 325 (2018), 326-327 (in questo saggio l'a. anticipa la più ampia indagine poi condotta in *The separation of platforms and commerce*, cit.). Pare andare in senso opposto a Google, invece, Facebook (anche se i servizi non paiono del tutto uguali) col prossimo servizio di *news*: P. Kafka, *Rupert Murdoch wanted Mark Zuckerberg to pay him for news stories — and now Facebook is going to do just that*, 24.10.2019, www.vox.com. In altre parole, questo ha serie ripercussioni anche economiche, in quanto l'oscuramento o la retrocessione nei risultati –determinati da criteri algoritmici del tutto sconosciuti e coperti da diritto d'autore- possono seriamente pregiudicare un'impresa. Tenta ora di rimediarvi il reg. UE 2019/1150 del 20.06.2019 sull'equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online: spt. imponendo l'obbligo di chiarire "i principali parametri che determinano il posizionamento e i motivi dell'importanza relativa di tali parametri principali rispetto ad altri parametri" (art. 5 § 1-§ 2 e cons. 24-27): che però mira a tutelare i soli "utenti commerciali" (imprese e professionisti, cioè i "professionisti" della normatva consumeristica: Palmieri A., *Profili giuridici delle piattaforme digitali*, cit., 20-21) e quindi non i "privati", tanto che si usa la sigla *P2B, platform-to-business* (AGCM-AGCOM-Garante Privacy,

Indagine conoscitiva sui Big Data, cit., p. 48); in ogni caso il rimedio dell'avviso all'utente, facendogli visionare la segnalazione del terzo (art. 5 § 4 del reg.), in caso di arretramento nei ranking o di oscuramento, sarà poco utile, dato che arriverà ex post (senza contraddittorio preventivo) e che non spiegherà il motivo (non richiesto) del perché ritiene di farla propria penalizzando l'utente (giudizio più positivo in Palmieri A., *Profili giuridici delle piattaforme digitali*, cit., 133; v. in questa opera anche le pagg. 109-126 sul posizionamento e sul ranking cioè sull'art. 5 del reg. cit). Analogamente v. alcune disposizioni della dir. UE 2019/2161 del 27.11.2019 di modifica della *consumer law* europea: ad es. l'art. 3, laddove inserisce il § 4 bis nell'art. 7 della dir. CE 2005/29, e l'art. 4, laddove inserisce l'art. 6 bis (e qui il § 1, lett. a) nella dir. UE 2011/83. Impone di comunicare le "informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato" nel caso di profiliazione e decisioni automatizzate il GDPR reg. 2016/679 (art. 13 c.2, lett. f; art. 14. c.2, lett. g; art. 15 c. 1, lett. h), con norme di complessa interpretazione (v. Wachter S.-Mittelstadt B.-Russell Ch., *Counterfactual explanations without opening the black box: automated decisions and the GDPR*, in *Harvard Journal of Law & Technology*, Spring 2018, vol. 31/2, 841 ss, sub V.A-B, 863 ss.); questi ultimi aa. tra l'altro ricordano a p. 863/4 che il cenno al diritto di spiegazione, presente nel cons. 71, non è stato riproposto nell'art. 22 (simile considerazione in Castets-Renard C., *Accountability of Algorithms in the GDPR and Beyondi*, cit., sub III.A.1, pp. 119-124, che nega la ricavabilità del *right of explanation* del singolo esito dal GDPR); anche se altra dottrina sminuisce il dato e opta invece con argomentazione di vasto respiro per il diritto ad una spiegazione (Noto La Diega G., *Against the Dehumanisation of Decision-Making*, cit., § 72), da intendere come spiegazione non solo della logica impiegata ex ante ma anche ex post, cioè relativa al singolo output che ha coinvolto l'interessato (Brkan M., *Do algorithms rule the world?*, cit., 110 ss.), anche per la strumentalità del diritto ad una piena spieegazione rispetto ad altri diritti del GDPR (rettifica e cancellazione, essenzialmente: Kaminski M.E., *The Right to Explanation, Explained*, cit., 213), il tutto però tenendo conto che per gli scienziati computazionali "*it's impossible to expect any useful form of general <explainability> for automated content selection systems*" (Stephen Wolfram, *Optimizing for Engagement*, cit., p. 7-8). E' stato pure osservato (Watcher S.-Mittelstadt, *A right to reasonable inferences: re-thinking data protection law in the age of big data and AI*, in *Columbia business law review*, 2019, 494 ss, lavoro molto approfondito) che la tutela contro le modalità di produzione e fruizione delle inferenze nei Big Data non è sufficiente nel GDPR (parte V, p. 542 ss) e nella sua applicazione da parte della Corte di Giustizia (parte IV, p. 521 ss), anche considerando <dato personale> le inferenze stesse (p. 515 ss; sarebbero infatti *economy class personal data*, p. 611): per cui gli aa. propongono di creare in via ermeneutica un (parzialmetne nuovo) specifico "right to reasonable inferences" (passim, spt. parte VI, 572 ss) ovvero a "right on how to be seen", p. 614. Oppure, stante l'insufficienza di una spiegazione *ex post*, si propone, da un lato, di dare maggior attenzione alla fase progettuale (data protection by design) e di redazione della valutazione di impatto ex art. 35 GDPR e, dall'altro, l'introduizione di audit esterni (Casey B-Farhangi A.-Vogl R., *Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise*, 34 *Berkeley Technology Law Journal 143* (2019), 179-183).

differenza dall'era televisiva[202], anche se qualcuno fa un parallelo con precedenti colossi aziendali come Standard Oil[203]), i quali possono tra l'altro liberamente modificare gli algoritmi che determinano i post (newsfeed) o i risultati che ciascuno riceve[204]; i social media infatti costituiscono <<the first significant speech forum in which a single "curator" controls both the production and receipt of speech by individual participants, determining simultaneously and continuously what each participant is allowed to say and to whom, and what speech each participant is allowed to receive, and how>>[205];

- alle loro enormi capacità di lobbying e di offrirsi come

[202] Magarian G.P., *Forward into the Past: Speech Intermediaries in the Television and Internet Ages*, cit., passim (ad es. p. 238, 253 e 255), ove paragone con la *television age*. Possibilità quasi illimitate di accesso non significa però libertà, secondo Yemini M., *The new irony of free speech*, cit.. L'a. distingue infatti la *capacity to speak*, certamente assai incrementata (Yemini M., cit., sub II e sopratutto sub II.A) dalla *liberty to speak*, che l'a. vede invece limitata in vario modo e precisamente in sei modi (Yemini M., cit., sub III.A.-F): i ruoli tecnici dei vari intermediari digitali, non vincolati dai limiti pubblicistici come è invece per lo Stato; nuove modalità di censura da parte dello Stato, tra cui proprio i safe harbour ex § 512 DMCA e § 230 CDA; seduction e manipulation da parte delle piattaforme; concentrazioni imprenditoriali nei new-media, mancanza di anonimato; lack of inviolability e cioè assenza del diritto di non essere zittito. Tuttavia il continuo paragone con l'era ante-internet non è così semplice: dato che oggi ci sono enormemente maggiori possibilità di comunicare, è ovvio che in termini assoluti siano aumentate le possibilità di censura (ci sono infatti tutte quelle che prima nemmeno erano concepibili). Bisognerebbe invece fare un paragone in termini relativi e cioè riferito al quantum di censura praticato rispetto al quantum di comuncazione possibile o messa in atto.

[203] Gorwa R., *What is platform governance*, in *Information, communication& society*, 2019, vol. 22/6, p. 860.

[204] Oltre a quanto osservato sopra alle note 151- 152 e testo corrispondente, v. Lev-aretz Y.-Strandburg K.J., *Privacy regulation and innovation policy*, in 22 *Yale j. l. & tech*. 256 (2020) 28, sub II.B-C, 267-271; G. De Gregorio, *Democratising online content moderation: A constitutional framework, Computer Law & Security Review*, 2019, 14.11.2019, 1 ss., 6-7 e 11 ; Origgi G., *La democrazia può sopravvivere a Facebook? Egualitarismoi epistemico, vulnerabilità cogniftica e nuove tecnologie*, Ragion pratica, 51, dicembre 2018, 445 ss (alla base dell'intelligenza collettive e dunque della "democrazia epistemica" dovrebbero stare: i) diversità di opinioni, ii) indipendenza, iii) decentralizzazione, iv) aggregazione: condizioni non soddisfatte dai social media attuali, p. 452 ss)

[205] Haan S.C., *Bad actors: authenticity, inauthenticity, speech, and capitalism*, in *Journal of constitutional law*, vol. 22/3, 2020, p. 623.

finanziatori di settori in crisi come quello giornalistico[206];

- alla equiparabilità di piattaforme come Facebook ai mezzi di informazione quanto ad efficacia informativa, anche se formalmente ospitante contenuti caricati dagli utenti, con conseguente (prima facie, almeno) inapplicabilità della relativa normativa editoriale[207];

- allo sfruttamento della vulnerabilità delle persone rilevata (in tempo reale, si badi[208], se non addirittura create ad hoc[209]) dal finegrained microtargeting tramite le innumerevoli tracce lasciate nel web[210] (sia quelle volontariamente lasciate che

[206] Feltri S., *If Journalists Want to Save Journalism, They Should Stop Asking Google for Money*, in https: //promarket.org, 23.10.2019.

[207] M. Monti, *Regolazione, Internet e tecnica*, cit., 27 ss, § 5.1-6; 2 Gillespie T., *Platforms Are Not Intermediaries*, in *Geo. L. Tech. Rev.* 198 (2018), passim, spt. 210-211: <<*We are now dealing with a third category: a hybrid between mere information conduits and media content providers, perhaps, or something new emerging from their convergence (…). they moved from delivering content for the person posting it to constituting it for the person accessing it. (…) As soon as Facebook changed from delivering a reverse chronological list of materials that users posted on their walls to curating an algorithmically selected subset of those posts in order to generate a News Feed, it moved from delivering information to producing a media commodity out of it*>> (per l'a. la *content moderation* è il servizio principale offerto, p. 201-202).

[208] I c.d. *bias* e le vulnerabilità vengono infatti rilevate e sfruttate in *real time*: Spencer S.B., *The problem of online manipulation*, in *Univ. of Illinois law review*, 2020/3, sub II.D.1.a-b, pp. 987-983.

[209] Spencer S.B., *The problem of online manipulation*, cit., 983; Khan L.M.-Pozen D.E., *A Skeptical View of Information Fiduciaries*, cit., p. 505 e 516 ss.

[210] Sieber A., *Souled out of rights? – predicaments in protecting the human spirit in the age of neuromarketing*, in *Life Sciences, Society and Policy*, 22.11.2019, vol. 15/1, § 4° e 5° (con toni particolarmente allarmistici); Susser D.-Roessler B.-Nissenbaum H., *Online Manipulation: Hidden Influences in a Digital World*, cit., tutto il saggio e specificametne sub V.B.2; v. ad es. p. 26: <<*part of what makes information technology particularly well-suited to facilitating manipulation is that it allows for finegrained microtargeting, making it possible for potential manipulators to engage in what Karen Yeung calls "hypernudging."92 Hypernudges are not only hidden, they precisely target and exploit individual vulnerabilities, making them much more difficult to resist*.>>; Zuboff S., *Il capitalismo della sorveglianza*, cit., 321-323. Le pratiche pubblicitarie manipolatorie da parte delle imprese naturalmente non sono nate oggi: negli Usa ad es. la Federal Trade Commission le ha perseguite sin dagli anni '50, anche se poi il vento è cambiato essendo prevalsa una visione "informativa" della pubblicità (così Woodcock R.A., *The Obsolescence of Advertising in the Information Age*, cit., 2272-2278 e poi parti I-II; l'a. discute in fine dei profili antitrust delle pubblicità tradizionali ancora oggi praticate, la cui funzione è tornata ad essere quella persuasiva, dopo l'assalto delle Big Tech: v. parte IV). La differenza delle due persuasività è però ovvia, visto che oggi, stante la rilevazione

quelle solo osservate o addirittura semplicemente inferite[211]), ultima fase evolutiva delle Big Tech secondo l'analisi di Zuboff[212], per cui può parlarsi di <<dynamical emotional targeting>>[213]) e alla capacità di condizionamento

dei dati personali, è mirata (diversa da soggetto a soggetto) e quindi assai più efficace: v. Spencer S.B., *The problem of online manipulation*, cit., per la contrapposizione tra la pre-digital Age (sub II.B, p. 966 ss) e l'attuale (sub II.C, p. 972 ss), e soprattutto Calo R., *Digital market manipulation*, 82 GEO. WASH. L. REV. 995 (2014), passim (il saggio spiega minuziosamente le ragioni della maggior efficacia dell'advertisment digitale odierno: personalizzazione spinta e maestria nell'uso delle cognizioni di behabvoral economics permettono di individuare e sfruttare le vulnerbilità dell'utente e i suoi bias cognitivi; p. 1041 ss discute le possibili scelte per porvi rimedio).

[211] Secondo la triplice distinzione posta dalle *Guidelines 08/2020 on the targeting of social media users* 02.09.2020 dell'European Data Protection Board, aperte alla discussione (sub cap. 5 *Analysis of different targeting mechanisms*). Un recente studio distingue tra *front-office customization* (trasparente, perché a beneficio dell'utente, tenendo conto delle sue preferenze) e *back-office customization* (opaca all'utente, perché a beneficio degli advertisers, rilevando dati dovunque e permettendo loro di selezionare –quindi sia includendo che escludendo- quelli da utilizzare per il targeting), la parte profittevole del business di Facebook (Haan S.C., *Bad actors: authenticity, inauthenticity, speech, and capitalism*, cit., p. 633 ss. e 656 ss., anche riportando indagini del sito investigativo *Propublica*).

[212] Quella che permette di cogliere gli stati d'animo e della personalità in genere: Zuboff S., *Il capitalismo della sorveglianza*, cit., ad es. in §§ 9.2-9.3, pp.284-305. Già ora si parla di *internet of bodies* per riferirsi ai devices da indossare, a fini sanitari ma non solo: si v. lo studio della McGill University per il World Economic Forum a firma di Xiao Liu, *The Internet of Bodies Is Here:Tackling new challenges of technology governance*, luglio 2020.

[213] Così Spencer S.B., *The problem of online manipulation*, cit., p. 979 (citando S. Fussel, *Alexa Wants to Know How You're Feeling Today*, the Atlantic del 12.20.2018). Qui v. anche indicazione dei brevetti di Amazon, Google ed IBM per rilevare lo stato d'animo o le emozioni negative tramite vari devices (rilevazioni del tono della voce ed altro: p. 979) e una definizione di manipolazione: <<*an intentional attempt to influence a subject's behavior by exploit-ing a bias or vulnerability*>>, p. 990. E' stato osservato che, a fronte di dichiarazioni ufficiali delle Big Tech a favore della *racial justice*, il loro business continua in realtà a prosperare sulle discriminazioni (Roose K., *Social Media Giants Support Racial Justice. Their Products Undermine It*, New York Times, 19.06.2020). E' dubbio se l'uso dei social produca dipendenza psicologica dagli essi: che l'astinenza sia dolorosa, è certo, per cui probabilmente un pò ne dà. Resta da vedere quanto, il che dipenderà anche (o largamente) dalle condizioni socio-economiche (e, in generale, personali) del singolo. Ravvisano tale dipendenza Banerjee A.V.-Duflo E., *Una buona economia per tempi difficili*, cit., 184-185; gli aa. tuttavia parrebbero addurre in senso contrario alla dipendenza il fatto che, in un esperimento, dopo conclusosi il mese di asistenza da social, i partecipanti chiedessero ancora di essere pagati per rinuncaire a Facebook: quando invece la circostanza mi pare provare la persistenza della dipednenza. Banerjee A.V.-Duflo

comportamentale (anche inconsapevole) propria della profilazione[214], essendo maestri nell'applicazione del nudge sulla base delle migliori conoscenze di behavioral science[215], anche se non mancano voci perplesse sulla reale capacità di precisione ed efficacia del microtargeting[216];

- alle incrementate possibilità di harassment via internet[217];
- all'opacità (anzi: totale oscurità) degli algoritmi, che non

---

E. la ravvisano alla luce dell'approfondito lavoro sperimentale di Allcott H.-Braghieri L.-Eichmeyer S.-Gentzkow M., *The Welfare Effects of Social Media*, *American Economic Review*, vol 110/3, 2020, pages 629-676, consultato in The National Bureau of Economic Research, che conclude così (dopo aver indicato alcuni aspetti positivi dei social): <<*Notwithstanding, our results also make clear that the downsides are real. We find that four weeks without Facebook improves subjective well-being and substantially reduces post-experiment demand, suggesting that forces such as addiction and projection bias may cause people to use Facebook more than they otherwise would. We _nd that while deactivation makes people less informed, it also makes them less polarized by at least some measures, consistent with the concern that social media have played some role in the recent rise of polarization in the US. The estimated magnitudes imply that these negative e_ects are large enough to be real concerns, but also smaller in many cases than what one might have expected given prior research and popular discussion*>> (§ 7 *Conclusion*).

[214] "*Behavioral deterrence or inhibitions, or so-called chilling effects, of profiling activities*": Büchi M.-Fosch Villaronga E.-Lutz C.-Tamò Larrieux A.-Velidi S.-Viljoene S., *The chilling effects of algorithmic profiling: Mapping the issues*, in *Computer law § security review*, 36 (2020), passim, spt. § 3. Il forte rischio di manipolazione è affrontato da Zarsky T.Z., *Privacy and manipulation in the digital age*, in *Theoretical inquiries in law*, 20/1, sub II,157 ss, passim, spt. 169 ss (fenomeno sempre esistito ma le cui conseguenze son ben maggiori in epoca digitale per l'opacità dei meccanismi e per la personalizzazione del messaggio, che lo rende più efficace: p. 171).

[215] Stemler A.-Perry J.E.-Haugh T., *The Code of the Platform*, *Georgia Law Review*, 2020, vol. 54/2, passim (spt. 622, 625 ss., 638 ss.). Suggerimenti per contrastare l'azione delle piattaforma in Lorenz-Spreen P.- Lewandowsky, S.-Sunstein, C.R-Hertwig R., *How behavioural sciences can promote truth, autonomy and democratic discourse online*, cit..

[216] Il colosso mondiale dei prodotti di largo consumo, Procter& Gamble, ha ridotto per questo la sua pubblicità su Facebook: Terlep S.-Seetharaman D., *P&G to Scale Back Targeted Facebook Ads*, in *The Wall Street Journal*, 17.08.2016 (sito web). V. pure Sloane G., *Why P&G decided Facebook ad targeting often isn't worth the money*, www.adage.com, 10 agosto 2016. Facebook ha in passato riconosciuto di aver sovrastimato le metriche di visualizzazione: Vranica S.-Marshall J., *Facebook Overestimated Key Video Metric for Two Years*, in *The Wall Street Journal*, 22.09.2016 (sito web).

[217] Suzor N.P., *Lawless. The secret rules that govern our digital lives*, cit., p.25 ss. e 46., per il quale evitare abusi e hate speeche costituisce la sfida maggiore per le piattaforme (p. 41).

permette né di conoscere la logica e i dati su cui operano né di rilevarne gli (inevitabili) errori[218] e ciò anche in termini di discriminazioni sociali (che proprio per questo sono assai meno percepibili rispetto a quelle proprie dell'era pre-algoritmica)[219] di vario tipo (ad es. pure l'età[220] o l'importanza sociale del soggetto, su cui bisogna decidere se keep up o invece take

[218] C.d. problema del *black box*, evidenziato da tutti gli aa., tra cui ad es. Castets-Renard C., *Accountability of Algorithms in the GDPR and Beyond: A European Legal Framework on Automated Decision-Making*, 30 *Fordham Intell. Prop. Media & Ent. L.J.* 91 (2019), sub IA, 96-104 oppure da Suzor N.P., *Lawless. The secret rules that govern our digital lives*, cit., p. 17 ss (per la content moderation). C'è una monografia sul tema, pure ricordata da tutti: Pasquale F., *The black box society*, cit. (del quale è interessante pure la parte sugli algorimti nel mondo finanziario, cap. 4, 101 ss). Da noi v. Bazzoni G., *La liberTà di informazione e di espressione del pensiero nell'era della democrazia virtuale e dei gloBal social media*, in *Diritto di internet*, 2019/4, p. 641. Se ne parla naturalmente anche a proposito dei contratti conclusi automaticamente: v. Sholz L.H., *Algorithmic contracts*, 20 *Stan. tech. l. rev*. 128 (2017), sub III.A (ad es. p. 152: <<*Where those who accept form contracts can be said to be "rationally ignorant," in black box algorithmic contracts there is no fixed set of things of to which a party can be said to be ignorant. What the algorithm is going to do is unknown to both parties*>>). Gli ostacoli a far valere l'accountability nell'algorithmic enforcement sono tecnici (opacità; imprevedibilità da machine learning), legali (copyright; segreti commerciali) e pratici (inefficacia della procedura di counter notification ex § 512.g.2.B DMCA) secondo Elkin-Koren N.-Perel M., *Algorithmic Governance by Online Intermediaries* (July 13, 2018), *Oxford Handbook of International Economic Governance and Market Regulation* (Eric Brousseau, Jean-Michel Glachant, & Jérôme Sgard Eds.) (Oxford University Press, 2018, Forthcoming), letto in ssrn.com, p. 14-16.

[219] Tra i molti aa. v. ad es.: Katyal S., *Private accountability in the age of artificial intelligence*, cit., sub I, p. 62 ss; Wacther S.-Mittelstadt-Russell C., *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*, 03.03.2020, in ssrn.com, 10-12, 48 e 67 (nel saggio gli aa.affermano la non completa algoritmizzabilità delle decisioni in tema di discrminazione e quindi propongo un loro metodo statistico che serva per una rilevazione *prima facie*, su cui poi intervenga però il giudice o il regolatore); più analiticamente in Wachter S., *Affinity Profiling and Discrimination by Association in Online Behavioural Advertising*, cit., passim (ad es. 9, 45/6, 54, 57, 68/71). Oppure Pasquale F., *The black box society*, cit., 38 ss. Ma il concetto di fairness nelle applicazioni algoritmiche è di difficile definizione: oltre a quanto indicato in nota 192, v. ad es. Hellman D., *Measuring algorithmic fairness*, in *Virginia law review*, 2020, vol. 106/4, p.846 ss e spt. 856 ss., per cui i riferimenti di genere o razziali non costituiscono necessariamente *disparate treatment* nel diritto USA.

[220] Alla discriminazione per età nei provvedimenti giudiziali è dedicato il saggio di Stevenson M.T.-Slobogin C., *Algorithmic Risk Assessments and the Double-Edged Sword of Youth*, in *96 WASH. U. L. REV. 681 (2018)*, che affermano –anche essi!- la necessità di maggior trasparenza degli algoritmi (v. III.B)

down[221]), magari in forma indiretta/occulta (c.d. proxy discrimination)[222] (anche se, adoperati all'inverso, gli algoritmi possono prevenire le discriminazioni)[223], opacità del modus operandi del'A.I. che è di per sé unfair[224], a poco servendo nei fatti gravare di responsabilità per danni i produttori di A.I. (sostanzialmente per prodotto difettoso) quando questa si basi su dati inaccurate oppure inappropriate[225] o è stata "allenata" male

[221] Kadri T.E.-Klonick K., *Facebook v. Sullivan: Public Figures and Newsworthiness in Online Speech*, 93 *South Cal. L. Rev. 37* (2019), sub III.B.3, 88-93.

[222] Che si ha quando il criterio usato per discriminare non lo è in sé ma solo indirettamente, in quanto l'utilizzatore sa che quel criterio gli permette le discriminazioni altrimenti vietate: ad es. rifiuta di vendere in certe aree geografiche –criterio in sé neutro- perché abitate da gruppi etnici con cui non intende stipulare contratti. Il tema è esaminato da Prince A.E.R.-Schwarcz D., *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 Iowa L. Rev. 1257 (2020), 1257 ss (l'esempio è tratto da p. 1269). Stanti gli errori inevitabili, è sorta una corrente di pensiero favorevole all'<<azione positiva>> algoritmica: v. Bent J.R., *Is Algorithmic Affirmative Action Legal?*, in *Georgetown law journal*, 2020, vol. 108/4, sub I.B, p. 814 ss (che si pone, superandoli, dubbi di legittimità, soprattuttto sul se ciò sia a sua volta discriminatorio, v. sub II.A e III.A). V. pure nota seguente.

[223] Kleinberg J.- Ludwig J., Mullainathan S.- Sunstein C. R., *Discrimination in the Age of Algorithms*, in *Journal of Legal Analysis*, Volume 10, 2018, Pages 113–174, § 6, 154 ss, e più sinteticamente ora in Kleinberg J.- Ludwig J., Mullainathan S.- Sunstein C. R., *Algorithms ad discrimintation detectors*, in *Proceedings of the National Academy of Sciences*, pnas.org, giugno 2020; Cofone I., *Algorithmic Discrimination Is an Information Problem*, in *Hastings law journal*, vol. 70/6, 2019, 1389 ss., precisando che più che bloccare certi dati (fonte di ulteriori problemi: sub III.A-B, 1416 ss), è meglio conformarli in positivo (*altering the data*) e cioè modificare i training data (shaping the data) oppure il codice del programma (*eocoding the data*: III.C-D, 1421 ss.). Risultano già applicati (c.d. discrminazione positiva) ad es. in Francia, USA e India: v. Piketty T., *Capitale e ideologia*, La nave di Teseo, 2020 (or.: 2019) 414-416 e 1145-1146.

[224] Sloane R.H.-Warner R., *Beyond Bias: Artificial Intelligence and Social Justice*, in *Virginia journal of law & technology*, vol. 24/1, 2020, III.C, 23 ss. Un'a. esperto della materia ha proposto di modificare le procedure di *content moderation* tramite l'applicaizone di "contesting algorithms" e cioè in sostenza applicativi del contraddittorio sulla base di un *adversarial public system* (*public AI* cioè *public artificial intelligence*), condizionando la legittimità del take down al superamento di tale scritinio *public AI* (Elkin-Koren N., *Contesting algorithms: Restoring the public interest in content filtering by artificial intelligence*, in Big Data & Society, 2020/2, p. 8-9). La proposta, oltre ad essere de jure condendo, è un pò vaga, non chiarendo a chi competerebbe la costruzione di questa tavola di valori confliggenti col diritto azionato (ad es. fair use), che per l'a. non può essere lasciata alla discrezione delle piattaforme.

[225] La responsabilità in tali casi è giustamente affermata da Pasquale F., *Data-Informed Duties in AI Development*, in *Columbia Law Review*, vol. 119/7, 2019,

o comunque è stata creata negligentemente secondo la scienza statistica e/o informatica;

- all'aumento notevole della diffusione di "bufale informative" (fake news[226]), anche nella versione più pericolosa delle deepfakes, quando consistono in falsi audiovisivi[227] (in

passim (ad es. 1919-1920 e poi pp. 1927/8, ove però sembrerebbe in ottica *de iure condendo*). Pasquale estende alla creazione di A.I. (e adatta alla bisogna) i doveri affermati a carico della struttura ospedaliera nel caso di responsabilità sanitaria *Thompson c. Nason Hospital* del 1991: << *(1) a duty to use reasonable care in the maintenance of safe and adequate facilities and equipment; (2) a duty to select and retain only competent physicians; (3) a duty to oversee all persons who practice medicine within its walls as to patient care; and (4) a duty to formulate, adopt and enforce adequate rules and policies to ensure quality care for the patients*>> (p. 1929-1931).

[226] Va in controtendenza Paglieri F., *La disinformazione felice*, cit., passim (libro interessante e di piacevole lettura). Secondo l'a., le bufale, esistite da sempre (porta alcuni esempi clamorosi) anche se in misura minore dato che minori erano i flussi informativi, non destano particolari timori (p. 137 ss.): basta avere un atteggiamento un po' critico ed anzi affrontarle direttamente per fare pratica dei giusti atteggiamenti epistemici (p. 177 ss e 233 ss sull'atteggiameno di *disintermediaizone felice*; anche se i noti *debunking* o *fact-cheking* son poco efficaci nei confronti dei <<bevitori di bufale>>: pp.145-156). C'è però da dubitare che simile impostazione, culturalmente critica, possa diffondersi tra il grande pubblico.

[227] Citron D.K.-Chesney R., *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 California Law Review 1753 (2019), sub II.B.1-2, p. 1771 ss (danni a soggetti individuali) e 1776 ss (danni alla società nel suo complesso), per cui, sulla base di precedente scritto di Citron, propongono una modifica del § 230 CDA che limiti il safe harbour per le deep fakes, onerando le piattaforme di provare di aver fatto *reasonable steps* per prevenire gli illeciti (p. 1799 ss.); Brown N.I., *Deepfakes and the weaponization of disinformation*, *Virginia journal of law & technology*, vol. 23/1, 2020, 1 ss., notizie per le quali i social sono l'ambiente ideale (*perfect storm*, p. 21-22). Questo a. segnala, da un lato, i seri pericoli per il *public trust* quando le gente non può credere nemmeno a ciò che vede, p. 11, e, dall'altro, che esistono però usi benefici delle deepfakes (a fini di satira e parodia, protetto dal Primo Emendamento, 32 ss.). Nonostante le dichiarazioni false godano della protezione del Primo Emendamento (Sunstein C.R., *Falsehood and the First Amendment*, in *Harvard Journal of law & technology*, vol. 33/2, 2020, 387 ss, passim, sub II, 396 ss.; R. L. Weaver, *Fake News (& Deep Fakes) And Democratic Discourse*, in *Journal pof technology law & policy*, vol. 24/1, 2019, 44 ss), la perdono (e sono quindi regolabili dal legislatore) quando possono causare seri danni ad individui o alla società nel suo complesso (Sunstein C.R., *Falsehood and the First Amendment*, cit., 392-396; Brown R.L., *The Harm Principle and Free Speech*, in *Southern California law review*, vol. 89/5, 21016, pp. 961/2, 992 ss e 999 ss, per la quale il danno legittimante l'intervento inibitorio è quello che non venga prodotto dalle mere idee; contrario R. L. Weaver, *Fake News (& Deep Fakes) And Democratic Discourse*, cit., 47 ss, tranne quando lo speech proviene dall'estero e mira a influenzare le elezioni statunitensi, p. 47/8; ritengono necessaria e legittima la

costante aumento per la crescente facilità informatica di loro creazione)[228] e della disinformazione in generale[229], che le piattaforme riescono ad affrontare in termini (non stranamente)

disciplina contro *fake news* e *false campaign speech* durante il processo elettorale Goldman A.I.-Baker D., *Free speech, fake news, and democracy, first amemdment law review*, vol. 18, 2019, 66 ss., sub V, p. 125 ss, ricorrendo i tre requisiti chiesti dall'importante sentenza *United States v. Alvarez* del 2012 e cioè i. rischio altrimenti di *legally cognizable harm*, ii. che il counter-speech non basti, iii. che sia la misura meno retrittiva per evitare il danno), tenuto poi conto che le notizie false si diffondono più veolcemente di quelle vere, impedendo il funzionamento corretto del c.d. *marketplace of ideas* (ivi, passim, ad es. p. 390, 393 e 406). Critica sulla soluzione di legislazione ad hoc per prevenire *fake news* anche Manzi D.C., *Managing the Misinformation Marketplace: The First Amendment and the Fight Against Fake News*, in *Fordham Law Review*, vol. 87/6, 2019, sub III, p. 2641 ss.: è improbabile che si possa predisporre una legge al tempo stesso efficace e compatibile col Primo Emendamento (p. 2648), per cui propone una restrizione all'accesso della professione giornalistica, per creare fonti informative qualificate, cui i cittadini possano rivolgersi (p. 2649-2650)..

[228] La Monaca J., *A Break from Reality: Modernizing Authentication Standards for Digital Video Evidence in the Era of Deepfakes*, in *American Law Review*, vol. 69/6, 2020, pp. 1955-1957 (che, circa l'attività di perseguimetno di questi falsi, scrive di <<*arms race between the creators and the detectors*>>, citando altro a.). La Monaca riferisce poi degli effetti (anche processuali) prodotti dall'esposizione ai fake video (op. cit., p. 1958 ss), che rende meno affidabili le deposizioni di testimoni o periti (p. 1980 ss).

[229] Pielemeier J., *Disentangling Disinformation: What Makes Regulating Disinformation So Difficult?*, in *Utah Law Review*, vol. 2020/4, 917 ss che così definisce *disinformation* (prendendo dalla Commissione UE): <<*"verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm.". (...) This definition covers deliberately spreading false news (often referred to as "fake news"), marketing products using false information, and distributing altered content (modified records, deep fakes, deceptively edited content or "shallow fakes," etc.). In some contexts, it may also include "blended" information (with elements of true and false content) and true information that is propagated with the intent to deceive the public, which is sometimes described as "propaganda" or "malinformation*.>>, p. 919; Yeargain T., *Fake Polls, Real Consequences: The Rise of Fake Polls and the Case for Criminal Liability Case for Criminal Liability*, in *Missouri law review*, vol. 85/1, 2020, p. 172 e 177 ss. sui falsi sondaggi elettorali) . Le piattaforme minori spesso non hanno le risorse per attuare contromisure informatiche all'altezza e devono quindi affidarsi alla moderazione degli utenti, come Reddit (op. ult. cit., p. 926). Altri utilizza il termine di *misinformation*, con cui indica l'informazione <<*that is "considered incorrect based on the best available evidence from relevant experts at the time"*>> (Bode L., *User Correction as a Tool in the Battle Against Social Media Misinformation*, in *Georgetown Law Technology Review*, vol. 4/2, 2020, 367, virgolettato nell'originale).

solo probabilistici[230]: il che produce minor credibilità nei media[231];

- alla violazione della privacy di una persona tramite l'aggregazione massiva di dati che la riguardano[232];

- alla possibilità di digital abuse, sempre più diffuso e la cui gravità è sottostimata[233];

- al fatto che sono le Big Tech a dettare le regole tecniche di cybersecurity, in assenza però dei consueti baluardi di difesa democratica (trasparenza, partecipazione, neutralità etc.) che

[230] V. Ananny M., *Making Up Political People: How Social Media Create the Ideals, Definitions, and Probabilities of Political Speech*, in *Georgetown Law Technology Review*, vol. 4/2, 2020, 351 ss, sub III.C, p. 362; Bode L., *User Correction as a Tool in the Battle Against Social Media Misinformation*, cit., sub II.A, p. 370 ss. (riferisce di due casi di rilevazione di *misinformation* in una discussione medica pari al 90,1 % e su Twitter pari al 95%, in media errori –falsi negativi- pari al 8,5 %).

[231] Carroll E. C., *How we talk about the press*, in *Gergetown law technology review*, vol. 4/2, 2020, 345. Per l'a., *fake news* è un ossimoro, dato che per *news* si intendono "*verifiable information in the public interest, and information that does not meet these standards does not deserve the label of news*" (p. 341, virgolette nel testo, riportando passo di altro a.). L'a., poi, segue la tesi della non invocabilità del Primo Emendamenot verso poteri privati (p. 344, ma senza approfondimento).

[232] Pike E.R., *Defending Data: Toward Ethical Protections and Comprehensive Data Governance*, 69 *Emory L. Rev*. 687 (2020), 703 ove si ricorda –p. 709- pure che il *privacy paradox* (la gente si dichiara preoccupata ma rarametne rifiuta i cookies o altri strumenti analoghi) e il *paradox of control*, per cui "the more that individuals believe they have control over their data, the more willing they are to share" (la parte I è dedicata ai pericoli derivanti dalla gestione dei *big data*). Sul *privacy paradox* c'è molta letteratura, tra cui ad es. ora v.: - Lutz C.-Hoffmann C.P.-Ranzini G., *Data capitalism and the user: An exploration of privacy cynicism in Germany*, in New Media&society, 2020/7, passim, spt. 1170 ss.; - Zarsky T.Z., *Privacy and manipulation in the digital age*, cit., 162 ss: Come sorge l'enorme asimmetria informativa tra le data-driven companies (DDCs) e i consumatori è spiegata da van de Waerdt P.J., *Information asymmetries: recognizing the limits of the GDPR on the data-driven market*, in *Computer Law & Security Review*, Vol., 38, September 2020, § 2.

[233] Kadri T.E., *Networks of empathy*, in *Utah law review*, vol. 2020/4, 1081-1082: l'a. propone sì maggior attenzione all'architettura degli algoritmi (1083 ss) e alla creazione o diffusione di norme sociali, p. 1097 ss ma prima di tutto suggerisce la necessità di approccio umano basato sull'empatia (soprattutto pp. 1078-1079). Sottolinea che i social sono diventati il principale mezzo di comunicazione tra le gang giovanili di Chicago, Curta N.F., *Unfriending The First Amendment: Social Media, Courts, And Juvenile Gang Members In Chicago.*, 69 De Paul L. Rev. (2020) sub I.B, p. 982-983.

operano quando il decisore è pubblico[234]. Discorso che va esteso all'artificial intelligence in generale, dato che, da un lato, la sua pervasiva diffusione regola ormai la vita delle persone in più sensi e lo farà sempre più, e, dall'altro, che gli algoritmi sottostanti sono sviluppati da enti privati, ai quali di fatto deleghiamo il comando di molte attività umane, senza che vi sia una loro corrispondente accountability[235].

[234] Suzor N.P., *Lawless. The secret rules that govern our digital lives*, cit., p. 90 ss. e, soprattutto, v. Kilovaty I., *Privatized cybersecurity law*, in *UC Irvine law review*, 2020 n. 6, sub III, 1211 ss. Nella parte I, Kilovaty ricorda il ruolo centrale in questo settore ricoperto da Microsoft tanto che un suo dirigente nel 2017, in un discorso allONU, propose di creare una Cyber Red Cross, analoga alla Croce Rossa a fini umanitari creata nel 1863 -col nome allora di International Committee of the Red Cross, ICRC-, per fronteggiare il problema di attacchi informatici sempre più massicci e devastanti. La cooperazione tra piattaforme, pur poco evidente dato che di solito esse trasmettono l'idea di competizione accesa per ridurre la pressione antitrust a proprio carico, è assai sviluppata in vari settori, tra cui la tecnologia per il filtraggio, dapprima su temi limitati (CSAM-child sexual abuse material) ma poi ad ampio raggio (GIFCT-global internet forum to counter terrorism; lotta alle campagne straniere di influenza politica; deepfakes che l'a. chiama *synthetic media*; il GIFCT si basa su un *hash database* segreto, come si legge in Gorwa R.-Bins R.-Katzenbach C., *Algorithmic content moderation: Technical and political challenges in the automation of platform governance*, in *Big Data & Society*, 2020, 2), detta *content cartel creep*, cartello strisciante sulla censura dei contenuti: v. Douek E., *The Rise of Content Cartels*, 11.02.2020, Knight First Amendment Institute-Columbia University, in knightcolumbia.org. L'a., pur notando i rimedi antitrust che mirano a ristgabilire la concorrenza non sono molto utili per affrontare i predetti temi (p. 15 ss del.pdf), individua comunque degli svantaggi da questi cartelli (Douek E., *The Rise of Content Cartels*, cit., p. 23 ss del.pdf): i) ulteriore riduzione di trasparenza, di due process e di accountability, ii) creazione di una apparente legittimazione sociale e di *progress*; iii) incremento del già enorme potere detenuto dalle piattaforme; iv) creazione di falsa apparenza su ciò che la società riterrebbe mediamente giusto passare o filtrare, mentre invece è frutto di accordo tra le piattaforme.

[235] Solow-Niedermann A., *Administering artificial intelligence*, in *Southern California law review*, vol. 93/4, 2020, sub III.A, p. 681-685: per risolvere il c.d. *public-private dilemma* (la delega agli enti tecnologici privati ha enormi problemi di accountability e indemocraticità; d'altro canto la regolazione pubblica ha problemi di lentezza e soprattutto di incapacità tecnologica), propone una sorta di via mezzo, consistente nel controllo pubblico sui fattori produttivi di questo business (computing power; human expertise; data) e sopratuttto su quello della selezione dei dati utilizzati (p. 687 ss). Evidenzia che, dopo il c.d. *digital divide*, si pone oggi un problema di *algorithimic divide* (relativamente a *awareness*, *access*, *affordability*, *availability* e *adaptability* delle applicazioni algoritmiche), Yu P.K., *The algorithmic divide and equality in the age of artificial intelligence*, in *Florida law review*, vol. 72, 2020, 331 ss: per l'a. alcune conseguenze indesiderabili (*algorithmic deprivation* e *algorithmic discrmination*) riguardano solo le fasce svantaggiate della popolazine, mentre la *algorithimc distortion*

Oppure pericoli legati alla regolarità della competizione economica, come quando l'algoritmo favorisce i prodotti della piattaforma –che è quindi in conflitto di interessi- rispetto a quelli degli altri venditori ivi ospitati (a caro prezzo)[236], combinato con l'effetto rete per cui il loro potere di mercato aumenta sempre più[237], dato che si avvalgono di tecnologie che per loro natura portano a dinamiche del tipo winner-takes-all[238];

riguarda tutti indistintamente (sub II). Soluzioni proposte dall'a. per ovviarvi (non particolarmente originali, per vero): *literacy, amelioration, ethics, transparency, accountability, competition* e *perspective* (cioè realismo ad ampio raggio, parrebbe) (sub III).

[236] Il software, che regola il marketplace di Amazon e soprattutto chi (uno solo dei tanti) -per un certo prodotto- può fruire della visibilità massima data dal comparire all'inizio con l'ambitissimo pulsante giallo a sinistra "aggiungi al carrello-acquista ora". Secondo Amazon, "*its Buy Box algorithm is a neutral arbiter designed to select the seller that best meets the needs of customers*" ma pare ci siano ampie prove in senso contrario e cioè nel senso che Amazon privilegia i prodotti che vende in proprio (cioè privilegia sé stessa): così S. Mitchell-S. Sussman, *How Amazon Rigs Its Shopping Algorithm*, promarket.org, 06.11.2019). Analoga preferenza per i propri prodotti viene praticata da Google nel servizio di acquisti comparativi: v. la sintesi della decisione 27.06.2017 con cui la Commissione UE accerta un abuso di posizione dominante ex art. 102 TFUE. Tenta di provvedere a questa *market failure* il reg. UE 2019/1150 del 20.06.2019 sull'equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online, spt. art. 7 *Trattamento differenziato*, e conss. 30-31. Aspetto che certo non permette agli accordi tra Amazon e i venditori sul suo *market place* di schivare la normativa antitrust (art. 101 TFUE), non potendosi più parlare di unica entità economica (Akman P., *Online Platforms, Agency, and Competition Law: Mind the Gap*, 43 Fordham Int'l L.J. 209 (Dic. 2019), sub VI, 295 ss, per il quale il rapporto tra loro è di *agency*). V. Bergqvist C., *Self-Favoring in the Digital Economy and the Role of Antitrust*, in promarket.org, 20 agosto 2020.

[237] Stemler A.-Perry J.E.-Haugh T., *The Code of the Platform*, cit., 615-622, passim. La necessità di *some sort of "digital authority" or regulatory agency to address both competition concerns and broader societal concerns* accomuna tre importanti recenti studi sulle piattaforme digiali (serie di paper dello Stigler Center dell'Univeristà di Chicago; uno studio per il governo del Regno Unito; ed uno per la Commissione UE-direzione Concorrenza, cit. pure infra): così riferisce Feld H., *From the Telegraph to Twitter: The case for the digital platform act*, in *Computer Law & Security Review*, 2020, vol. 36, p.1 (ove link ai documenti).

[238] Acemoglu D.-Robinson J.A., *La strettoia. Come le nazioni possono essere libere*, Il Saggiatore, 2020 (orig.: 2019), p. 644 ss ; <<grazie agli effetti di rete, una tendenza verso la monopolizzazione è nel DNA delle piattaforme>> (Srnicek N., *Capitalismo digitale*, cit., p. 82-84 e 85 ss.; e grazie pure alla possibilità di sovvenzioni incrociate: ivi, p. 103). I pericoli maggiori per il corso azionario per Facebook sono il rischio di regolazione, da un lato, e la perdita di utenti per mutamento nei *social media* trends (nelle mode, in sostenza), ciò che sta già avvenendo (così Öhman C.-Aggarwal N., *What if Facebook goes down? Ethical*

o come quando si sfruttano i consumatori con discriminazioni di prezzo, tramite l'estrazione del c.d. surplus del consumatore, dato che il microtargeting permette di individuare con una buona precisione il massimo che egli è disposto a spendere[239]; o infine i pericoli per il calo di innovazione tecnologica nel caso che le big platforms acquistino le più interessanti start-up, anziché lasciarle prosperare e acquisire la loro tecnologia dal mercato secondario[240]. Ed anzi le Big Tech cercano di incrementare il loro già enorme potere, facendo lobbing sui governi per la stipula di accordi internazionali sul digital trade del tipo di quelli alla base della Word Trade Organization[241], per non dire di altre conseguenze assai dannose (poco note) legate al forte contributo dato al surriscaldamento globale[242]. Del resto, le collettività nel corso della storia hanno spesso cercato di impedire la

and legal considerations for the demise of big tech, in *Internet Policy Review*, vol. 9/3, 2020, p. 3).

[239] Stiglitz J.E., *Popolo, potere e profitti*, Enaudi, 2020 (orig.: 2019), p. 66 e p. 129. Il Parlamento UE ha di recente invitato la Commissione a muoversi per far escludere il micro-targeting dalle piattaforme (*European Parliament resolution of 18 June 2020 on competition policy – annual report 2019*, § 105)

[240] Nel lungo periodo, infatti, le imprese maggiori tendono a perdere la loro forza innovatrice, per cui è preferibile conservare un vivace mercato composto anche da piccole imprese (Merges R.P., *Patent markets and innovation in the era of big platform companies, in Berkeley tech. law journal*, vol. 35/1, 2020, spt. sub I a p.55 ss., e sub III, p. 81 ss.). Simile linea di pensiero in Lemley M.A.-McCreary A., *Exit Strategy*, in *Stanford Law and Economics Olin Working Paper #542*, letto in ssrn.com, sub III, soprattutto III.A-B, pp. 51-60, e in Katz M.L:, *Big-Tech Mergers: Innovation, Competition for the Market, and the Acquisition of Emerging Competitors* (July 21, 2020), letto in ssrn.com (in termini anche matematici). V. pure Scott Hemphill C., *Disruptive incumbents: platform competition in an age of machine learning*, in Columbia law review, 2019, vol. 119/7, 1974 ss (sulla barriera all'entrata costituita dalle tecnologie c.d. *macbine learning*)

[241] V. l'analitico esame della proposta di *digital trade rules* in James D., *Digital trade rules. A disastrous new constitution for the global economy, by and for big tech*, in cepr.net, luglio 2020 (v. ad es. il § iniziale *History and status of the proposed digital trade rule*, p. 10-18 oppure la sintesi con pari titolo sempre in cepr.net, 08.07.2020).

[242] E' purtroppo poco diffusa la consapebolezza che lo storage degli enormi data center richiede un immane quantità di energia e la dottrina parla di *data waste* (Bietti E.-Vatanparast R., *Data waste*, in *Harvard international law journal. Frontiers*, Vol. 61/2020, con riferimento alle *data-driven infrastructures* che includono "platform-based business models, the programming and use of AI systems, and blockchain-based technologies" (pp.2-3). V. similmente Brevini B., *Black boxes, not green: Mythologizing artificial intelligence and omitting the environment*, in Big Data & Society, 2020/2, pp. 3-4.

formazione di poteri privati troppo ampi[243].

Tutto questo, però, non rileva nel caso nostro, ove il legislatore ha voluto riservare il safe harbour a chi non sa dell'illiceità (e a chi sa, ma subito ha proceduto a rimuovere i contenuti e/o disabilitare l'accesso): situazione circa la quale la struttura oligopolistica in sé del mercato degli intermediari poco o nulla dice. Le pur serissime preoccupazioni per il tasso di democraticità e per la trasparenza dei processi politici, non è con questo corpus normativo che vanno affrontate.

12. Intermezzo su una recente e nota sentenza di Cassazione

Secondo una recente opinione giurisprudenziale, <<*la distinzione tra hosting provider attivo e passivo può, a ben vedere, agevolmente inquadrarsi nella tradizionale teoria della condotta illecita, la quale può consistere in un'azione o in un'omissione, in tale ultimo caso con illecito omissivo in senso proprio, in mancanza dell'evento, oppure, qualora ne derivi un evento, in senso improprio; a sua volta, ave l'evento sia costituito dal fatto illecito altrui, si configura l'illecito commissivo mediante omissione in concorso con l'autore principale. La figura dell'hosting provider attivo va ricondotta alla fattispecie della condotta illecita attiva di concorso. (…) Dunque, si può parlare di hosting provider attivo, sottratto al regime privilegiato/ quando sia ravvisabile una condotta di azione, nel senso ora richiamato*>>[244]. L'affermazione lascia perplessi, laddove par dire che l'hosting provider, quando è "attivo", diventa automaticamente concorrente nell'illecito. Si confondono due piani diversi: A) il concorso nel singolo illecito sub iudice; B) la modalità di svolgimento (in generale, non nel caso sub iudice) della propria attività da parte dell'internet provider, per capire se può fruire o meno del safe harbour. La distinzione tra provider attivi e passivi ha a che fare col secondo piano, sub B), mentre non ha nulla a che fare col primo. In altre parole, il fatto, che un provider sia qualificato come attivo, non

[243] Questo aspetto percorre ampie parti del libro di Acemoglu D.-Robinson J.A., *La strettoia. Come le nazioni possono essere libere*, cit.: v. ad es. dove gli aa. ricordano l'istituto dell'ostracismo nella Grecia antica, che colpì pure Temistocle, artefice della potenza navale ateniese ed eroe nelle guerre contro i Persiani e quello simile presso la popolazione africana dei *Tiv*.

[244] Cass. 19.03.2019 n. 7708 cit., § 4.3.

significa che gli si possa per ciò solo addebitare il concorso con l'utente in un certo illecito.

Come sopra ricordato, il concorso fonte di (cor-)responsabilità civile[245] prevede un contributo in termini causali nella produzione dell'evento di danno portato in giudizio: circa l'accertamento di quest'aspetto fattuale, però, solitamente nulla può segnalare che il business condotto dal provider sia strutturato o meno con le attività di filtro/suggerimento/indicizzazione etc. che i giudici utilizzano per ravvisare il ruolo attivo[246]. Bisognerebbe provare che tale modello di business avesse causato o contribuito a causare – anche solo in termini probabilistici- la specifica violazione sub iudice: prova a priori impossibile se per "violazione" si intende il mero uploading e comunque difficilissima (probabilmente impossibile, almeno per il soggetto leso) anche se per "violazione" si intendono dowloading, condivisione, linking e simili.

Inoltre la distinzione tra illecito omissivo proprio e improprio è di dubbia trasponibilità nella responsabilità civile: questa esiste solo in caso di contributo causale (omissivo o commissivo non conta: nel primo caso omissione c.d. impropria) alla produzione di un danno, mentre non rileva la mera violazione del dovere di attivarsi cioè l'astensione in sé a prescindere da un danno (omissione c.d. propria).

13. Il provider di mero trasporto (art. 14 d. lgs. 70/2003). L'inibitoria/injunction

Per l'attività di semplice trasporto, che comprende pure il dare

[245] Diverso è il discorso per gli altri rimedi all'illecito. Le inibitorie riguardano la sola condotta dell'ingiunto, per cui non si pone un problema di concorso, la cui pecualiarità in pratica consiste nell'applicazione della responsabilità solidale.

[246] Secondo la cit. Cass. 7708/2019, <<*gli elementi idonei a delineare la figura o "indici di interferenza" da accertare in concreto ad opera del giudice del merito, sono – a titolo esemplificativo e non necessariamente tutte compresenti – le attività di filtro, selezione, indicizzazione1 organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione dei contenuti/ operate mediante una gestione imprenditoriale del servizio, come pure l'adozione di una tecnica di valutazione comportamentale degli utenti per aumentarne la fidelizzazione: condotte che abbiano/ in sostanza/ l'effetto di completare ed arricchire in modo non passivo la fruizione dei contenuti da parte di utenti indeterminati*>> (§ 4.3, in fine).

accesso alla rete (art. 14 d. lgs. 70/2003)[247], il provider non è responsabile se i) non dà origine alla trasmissione[248], ii) non seleziona il destinatario, iii) non seleziona ne modifica le informazioni trasmesse[249]. Sono i profili, che concretizzano per questo tipo di provider quel ruolo di passività e automaticità di servizio appena visto e indicato dal cons. 42 dir. 2000/31. In effetti, se vuole qualificarsi come provider di mero trasporto/mero accesso non può -lo si comprende- porre in essere azioni rientranti nei tre tipi indicati dalla legge: non sarebbe più un provider di mero trasporto, in quanto sarebbe lui a dare almeno in parte la direzione (o il contenuto) alla attività comunicativa inizialmente realizzata dall'utente. Il safe harbour allora verrà meno e si applicherà la disciplina di diritto comune: probabilmente ci sarà un concorso del provider con l'utente uploader[250].

Il comma 2 fornisce una specificazione, della quale non ci sarebbe stato bisogno, dal momento che anche questa memorizzazione automatica e transitoria, se necessaria al funzionamento del servizio, doveva comunque essere ritenuta irrilevante ai fini della fruizione delle esimente. Piuttosto è

[247] Sulla duplicità di fattispecie e sulla ragione del loro apparentamento nel medesimo articolo v. Bocchini R.,, *La responsabilità civile degli intermediari del commercio elettronico*, cit., 132-133. L'a. nota che la L. delega 01.03.2002 n. 39, art. 31, lett. d), aveva menzionato solo il trasporto, omettendo l'accesso, e ricorda che sono molti in rete gli operatori che svolgono funzioni di *mere conduit*: computer routers, gateways etc. (p. 133 e nota 3 a p. 20).

[248] E' l'utente che deve darvi inizio con l'atto di uploading del file o del post sulla piattaforma. E' quindi inesatto dire che la disposizione non va intesa in senso letterale, perché sarebbe sempre il provider a darvi inizio (Montagnani M.L., *Internet, contenuti illeciti e responsabilità degli intermediari*, cit., 89, alla cui pag. seg. trovi l'interessante questione dei c.d. black hole informatici per i mere conduit providers, i quali, essendo in sostanza frutto di attività di filtraggio, potrebbero violare la lett. b) o c) della relativa disciplina).

[249] Si è precisato che il provider non deve essere l'autore delle informazioni (Riordan J., *The liability of internet intermediaries*, cit., 395, sub 12.83): questo, pur non previsto espressamente (come ad es. all'art. 14 § 2 dir. 2000/31), deriva implicitamente dal dettato del c. 1 ("informazioni fornite da un destinatario del servizio") e comunque costituisce il presupposto generale del safe harbour. L'a. poi esamina la qualificazione di alcuni tipi di provider o di loro condotte, come ad es. i VPNs, proxies e DNS server o quando blocca il traffico (pp. 396/7).

[250] Secondo Bocchini, *La responsabilità civile degli intermediari del commercio elettronico*, cit., 137/8, invece, ci sarà sempre un concorso, secondo la sua teoria, per cui il safe harbour non delinea solo una sottrazione alla disciplina generale, ma un'alternativa alla correponsabilità.

interessante l'esplicitazione –anche se pur essa non sarebbe a questo punto necessaria- che la memorizzazione automatica debba essere limitata al tempo "ragionevolmente" (non "strettamente", ad es.) necessario[251] all'esecuzione della trasmissione (c.2): una memorizzazione maggiore esorbita dal ruolo passivo e neutro. Il che anticipa ciò che rileva pure nel cahing provider, anche se ivi non è detto con questa precisione, ma è comunque ricavabile (c. 1: "effettuata al solo scopo di rendere più efficace il successivo inoltro"; v. anche lett. c) e lett. e))[252].

Secondo il c. 2, il safe harbour è concesso anche per le attività di memorizzazione temporanea, dettate da ragioni solo tecniche (anche in termini temporali) per le miglior esecuzione del servizio. Nulla dice più di quello che sarebbe stato ricavabile dal c. 1 in base ad ordinaria interpretazione teleologica[253], anche se così si evitano fastidiose discussioni.

Il c. 3 contiene una regola, che si ripete quasi identica[254] anche nelle altre tipologie di provider (art. 15/2 e art.16 / 3), e dunque ne accenno qui. Si fa salva la possibilità che l'autorità (giudiziaria o amministrativa con funzioni di vigilanza: su quest'ultima sarebbe interessante ragionare per individuarla compiutamente[255]) esiga che il prestatore delle tre tipologie

[251] <<reasonably necessary>>, <<raisonnablement nécessaire>>, secondo le versioni della dir. (fa riferimento alla prassi la versione tedesca: <<als es für die Übermittlung üblicherweise erforderlich ist.>>).

[252] Secondo un a., non è prevista la fattispecie per cui il provider conosce i materiali transitati ma con rispetto dei tre requisiti di esenzione (Bocchini R.,, *La responsabilità civile degli intermediari del commercio elettronico*, cit., 137). Direi che il safe harbour opera senza problemi: il paragone con la disciplina delle altre due tipologie di provider porta a questa conclusione.

[253] Conf. Bocchini R., *La responsabilità civile degli intermediari del commercio elettronico* cit., 131-2, ove si ricorda che pure questa regola era stata omessa dai criteri direttivi della l. delega.

[254] E' identica rispetto al'art. 15 c. 2, mentre c'è una differenza di dettato rispetto all'art. 16 c.3: per il mere conduit e il caching provider si dice <<l'autorità giudiziaria o quella amministrativa aventi funzioni di vigilanza>>, mentre per l'hosting provider si dice <<L'autorità giudiziaria o quella amministrativa competente>>. Non pare dubbio però che anche nell'ultimo caso la competenza debba sussistere in relazioni a fini di vigilanza, non vedendosi per quale altra funzione amministrativa possa ordinarsi la cessazione o la prevenzione. Quindi la differenza testuale dovrebbe svanire in sede interpretativa.

[255] Secondo Cons. St., sez. VI, 15.07.2019 n. 4993, sub § 7.2.1.c.1, che ha posto fine alla lite intorno alla legittimità del Regolamento AGCom sulla tutela del diritto d'autore ininternet (delibera 680/13/CONS del 12.12.2013), è proprio

impedisca o ponga fine alle violazioni commesse o meglio che "in quel momento" risultino commesse (l'ordine può infatti anche essere messo in via d'urgenza id est solo cautelare). Si tratta dell'inibitoria cioè di quel provvedimento che proibisce un certo comportamento: in particolare, di proseguire quello in atto oppure di tenerlo (di nuovo o per la prima volta) in futuro. Nella fattispecie, può attuarsi nella dualità comportamentale menzionata della rimozione dei materiali (le informazioni) o -a monte- della disabilitazione dell'accesso: questo quanto al por fine alla violazione commessa. Quanto all'impedimento per il futuro, consisterà nell'implementare (oppure nell'utilizzare in modo appropriato se già ne dispone) i software (cosiddetti filtri) che individuano i materiali -allo stato- ritenuti illeciti. Si tratta in sostanza di una misura con finalità non sanzionatoria ma collaborativa[256].

La norma ripete pari pari quella corrispondente della direttiva, a parte il riferimento alla possibilità di disporlo anche in via

l'AGCom l'Autorità, cui si riferiscono le norme citate (non viene menzionato però l'hosting provider). Tale sentenza afferma la sufficienza di base normativa per i poteri normativo-regolametnari in capo all'AGCom (§ 7.2) e l'insufficienza invece per i poteri sanzionatorio-pecuniari nel caso di inottemperenza (§ 20). Da un lato, però, potrebbe forse dirsi che il potere di vigilare, accertare ed emettere ordini comportasse implicitamente pure quello di creare sanzioni (contra il C.d.S. al cit. § 20); dall'altro, che i due profili non possono distiguersi sotto il profilo del rispetto del principio di legalità, dato che l'art. 23 Cost. lo pone sia per la <<prestazione patrimoniale>> sia per quella <<personale>>, tra cui rientra certamente (sul punto v. L. Antonini, Art. 23, in *Comm. alla Cost.* dir. da Bifulco-Celotto-Olivetti, Utet, 2006, 1, sub § 2.2., 491-492). Il punto principale (ormai solo a livello teorico) è che resta incerta la base giuridica anche per i poteri regolamentari, affermata invece dal CdS (v. § 7.2.1). Il tema è complesso e farò solo pochi cenni. E' alquanto generico l'art. 182 bis l. aut., che non cita i servizi internet: né può trovarsene la ragione nel fatto che si tratta di norma troppo risalente nel tempo, dato che - i) la dir. 2000/31, del medesimo anno di introduzione dell'art. 182 bis, menziona espressamente l'internet più volte nei Considerando); e - ii) a monte, ciò non è comunque motivo per eludere il principio di legalità. Inoltre nemmeno è invocabile la teoria dei c.d. poteri impliciti, dato che, mentre questa prevede il riconoscimento di poteri non espressamente attribuiti per permettere il proficuo esercizio di quelli espressamente attribuiti (v. la voce *McCulloch v. Maryland-law case* nell'*Encyclopaedia Britannica*; v. art. 352 TFUE che però li prevede espressamente a livello costituzionale europeo), nel caso de quo è dubbia anche l'assegnazione dei primi cioè di quelli asseritamente assegnati in modo esplicito (per cui sarebbero "impliciti al quadrato"!).

[256] Costituiscono un *cooperation tool* e non un *tool of sanction*, secondo M. Husovec, *Injunctions aganist intermediaries in the European Union*, cit., 60 ss.: si può convenire con l'affermazione.

d'urgenza: precisazione poco utile, poiché se l'inibitoria è ammessa in via definitiva, non si vede come la si possa escludere in via cautelare (tale essendo la via d'urgenza)[257]. Essa vuole dire che, anche se il provider fruisce delle esenzione da responsabilità, ciò nonostante può essere soggetto ad inibitoria (v. pure cons. 45). L'affermazione è pacifica, alla luce del dettato normativo[258], e conferma che la reazione all'illecito non consiste solo nella responsabilità, nel senso di risarcimento del danno, ma anche in altre misure, la principale delle quali è appunto l'inibitoria[259]. Non ci sono particolari problemi nell'interpretare il contenuto dell'inibitoria: la legge è sufficientemente chiara nel senso che deve trattarsi di cessazione o prevenzione relativamente a specifici[260] materiali ovvero –

[257] Nella proprietà intellettuale non si dubitava della opposta possibilità della ammissibilità dell'inibitoria definitiva, quando era prevista solo quella cautelare; né i suoi effetti non erano del tutto deducibili dala sentenza di accertamento dell'illecito (relativo a fatti passati), servendo pure uno specifico capo per l'ordine inibitorio (per fatti futuri) (Vanzetti M., *Contributo allo studio delle misure correttive e delle sanzioni civili nel diritto industriale: i profili processuali dell'art. 124 c.p.i.*, in *Riv. dir. ind.*, 2010, 37 ss). Nemmeno vi ostava il fatto che la non perfetta corrispondenza di comando tra il provvedimenot cautelare e quello definitivo, essendo ovvio che il primo riguarda solo i comportamenti conseguenti al futuro accertamento di illiceità e non l'accertameno in sé, che può essere contenuto solo nel comando definitivo (Spolidoro M.S., *Le misure di prevenzione nel diritto industriale*, Giuffrè, 1982, p. 195 ss): in realtà pure la cautela contiene un accertamento, ma finalizzato solo alla cautela stessa e dunque inidoneo al giudicato (anche se dotato di maggior stabilità dopo l'attenuazione del nesso di strumentalità provocatga dal c. 6 dell'art. 669 octies cpc).

[258] Una mongrafia specifica sul punto è quella di M. Husovec, *Injunctions aganist intermediaries*, cit., spt. pp. 58-59. Lo specifica l'AG Szpunar nel caso C-18/18, Eva Glawischnig-Piesczek c. Facebook, § 32 e da noi ad es. Trib. Mi ord. 12.04.2018, *Mondadori c. Fastweb e altri*, in *Dir. di internet*, 2018/1, 110.

[259] Si ricordi che secondo una nota ed argomentata tesi, rimasta però sostanzialmente isolata, l'inibitoria non è altro dall'accertamento dell'illecito (Spolidoro M.S., *Le misure di prevenzione nel diritto industriale*, Giuffrè, 1982, capo II, passim, spec.. p. 81 ss). Tema complesso è quello del se l'inibitoria costituisca rimedio generale e cioè esperibile oltre i casi in cui è espressamente prevista: si, per Trimarchi P., *La responsabilità civile: atti illeciti, rischio, danno*, Giuffrè, 2017, p. 543, per analogia con i casi già previsti (ma ciò è ovvio ex art. 14 prel., tranne che se ne affermi la natura di norme eccezionali: giudizio che dovrà allora riguardare ciascuna disposizione), e per Nardo G.N., *Profili sistematici dell'azione civile inibi-toria*, Napoli, 2017, p. 85 (ove ampio esame critico della dottrina in materia: p. 75 ss.).

[260] La specificità non risulta testualmente ma indirettamente: dal divieto di sorveglianza generale, a sua volta dalla impossibilità di comprimere l'autonomia privata e di impresa dei privati, che ha pure copertura costituzionale, alla luce

come è stato sintetizzato- deve avere carattere cooperativo e non sanzionatorio[261].

Non affronto invece per problemi di spazio il tema della parte su cui debbano ricadere i costi d'implementazione dei filtri, anche se importante nella pratica e oggetto di diverse soluzioni a livello europeo[262]. La normativa europea tace, mancando sia disposizione esplicita che norma implicita: né quest'ultima è ravvisabile nel secondo periodo del cons. 59 dir. 2001/29 (<<In molti casi siffatti intermediari sono i più idonei a porre fine a dette attività illecite>>), che si riferisce al fatto che sono gli intermediari ad avere il controllo tecnologico e contrattuale dei materiali caricati[263]. Il punto, come in genere la disciplina contenutistica dell'inibitoria, sarà allora regolato dai diritti nazionali e lo si desume pure dall'ultimo periodo del cons. 59 dir. 2001/29 (<<Le condizioni e modalità relative a tale provvedimento ingiuntivo dovrebbero essere stabilite dal diritto nazionale degli Stati membri>>) e dall'analogo dictum (non si può scrivere "regola", "disposizione" etc.) del secondo periodo

dell'art. 23 Cost. (v. Fedele A., Art. 23, in De Siervo U.-Fedele A., Art. 22-23 *Rapporti civili*, in Branca (a cura di), *Commentario della Costituzione*, Zanichelli-Il Foro italiano, 1978, § 15, p. 126 ss). Tuttavia, secondo l'a., per le prestazioni patrimoniali prevale la ratio di soddisfazione di interessi generali, mentre il profilo garantistico è centrale per le prestazioni personali.

[261] Così M. Husovec, *Injunctions aganist intermediaries*, cit., 60 e 57-64 con argomenti a favore. Parla di cooperazione pure l'AG Szpunar in Ziggo C-610/15, << *Orbene, le deroghe in materia di responsabilità dei prestatori intermedi previste dalla direttiva 2000/31 costituiscono uno degli elementi dell'equilibrio tra i vari interessi in gioco che rappresenta tale direttiva, ai sensi del considerando 41 della stessa. Tali deroghe, nell'ambito di tale equilibrio, devono essere controbilanciate non solo dall'assenza di complicità dei prestatori intermedi nel violare la legge, ma anche dalla loro cooperazione al fine di evitare o prevenire tali infrazioni*>>, § 13.. E a precisazione del fatto che la cooperazione richiesta è nei termini posti dal giudice o dall'autorità, aggiunge: <<*Essi non possono sottrarsi a tale obbligo invocando, in funzione delle circostanze, né il carattere troppo restrittivo delle misure, né la loro inefficacia*>>), § 83 (con errore di numerazione nel sito web C.G. nella versione italiana).

[262] Sono a carico del provider in Francia e nelle sentenze *Sabam* e Telekabel della C.G.; restano a carico del soggetto leso in UK (Geiger Ch.-Izyumenko E., *Blocking Orders: Assessing Tensions with Human Rights*, 2019, in Frosio G. (ed.), *The Oxford Handbook of Intermediary Liability Online*, OUP, 2020, Forthcoming, letto in ssrn.com, p. 16-17).

[263] Pare invece pensarla all'opposto O'Sullivan, Kevin T., *Copyright and Internet Service Provider 'Liability': The Emerging Realpolitik of Intermediary Obligations'*, in *IIC-International Review of Intellectual Property and Competition Law*, 2019, 550-552, §§ 20-21.

del cons. 23 dir. 2004/48 (uguale al prec., tranne che per la sostituzione del termine <<ingiuntivo>> con <<inibitorio>>)[264]. La disciplina contenutistica europea sul punto pare limitarsi ai vaghissimi criteri (nemmeno clausole generali, direi, dato che è difficile individuare gli standard di rinvio), posti dall'art. 3 dir. 2004/48 § 1 e 2 per le <misure e procedure>, concetto nel quale le ingiunzioni rientrano[265], nonché –come al solito- nel limite della non incompatibilità col diritto UE.

I casi reali discussi di access-mere conduit sono pochi. Ricordo Mc Fadden c. Sony[266], in cui la C.G. ha così qualificato la messa a disposizione del pubblico di una rete wifi all'interno (forse anche all'esterno) di un negozio da parte del titolare. La Corte ha detto che: i) nessun altra condizione è richiesta per l'applicazione dell'art. 12 dir, oltre a quanto espressamente ivi richiesto: in particolare non è necessario un rapporto contrattuale ad hoc né che sia stata fatta pubblicità di questa iniziativa (§§ 44-54); ii) il dovere di prevedere l'immediata rimozione/disabilitazione -ex art. 14 § 1 lett. b)- non è applicabile per analogia a detto tipo di internet provider (§§ 62-65; più per impossibilità tecnica che per esclusione di principio, parrebbe); iii) il soggetto leso può chiedere al provider la rimozione/disabilitazione, ma non un risarcimento del danno o rimborso di spese legali (§ 79); iv) è compatibile con l'art. 12 (e con le dir. 2001/29 Infosoc e 2004/48 c.d. enforcement) un'inibitoria, che lasci la scelta della misura restrittiva al fornitore di accesso, anche se questa poi si limita ad imporre una password agli utenti, però << nei limiti in cui gli utenti di detta rete siano obbligati a rivelare la loro identità al fine di ottenere la password richiesta e non possano quindi agire anonimamente,

[264] il punto è pacifico. V. comunque: - M. Husovec, *Injunctions aganist intermediaries in the European Union*, cit., 94 ss; - Petruso, R., *La responsabilità degli intermediari della rete telematica*, cit., 146; - C.G. 27.03.2014, *UPC Telekabel c. Constantin Film+1*, C-314/12, §§ 43-44; - Conclusioni AG Szpunar sia in C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, § 33, che prima in *Tobias Mc Fadden c Sony Music Entertainment Germany GmbH*, C-484/14, § 85.

[265] Non rientrano invece nel concetto di "sanzione" posto dall'art. 8 § 1 dir. 2001/2, stante la contrapposizione tra § 1 e § 3. Dunque per questa via non si applicherebbe alle inibitorie il criterio del § 1 per cui devono essere <efficaci, proporzionate e dissuasive>; tuttavia lo si applica per altra via, essendo stato recepito tale e quale dal cit. art. 3 dir. 2004/48.

[266] C.G. 15.09.2016, C-484/14.

circostanza che spetta al giudice del rinvio verificare>> (5°, 9° e 10 ° questione pregiudiziale, §§ 80 ss, spt. § 101)[267].

E' stata affermata la natura "speciale" della disciplina del mere conduit, stante il favor ivi contenuto: con la conseguente inapplicabilità analogica a casi non previsti[268]. Ora, intendendo "speciale" come "eccezionale" ex art. 14 preleggi, la peculiarità della disposizione (che arrivi al punto della eccezionalità ex art. 14 prel., è da vedere) parrebbe stare nel fatto che, per fruire del safe harbour, chi presta questo tipo di servizio internet può limitarsi a provare il (non) ricorrere dei tre requisiti posti dal c. 1 e niente più. In particolare è esclusa una valutazione della sua condotta in termini di colpa/negligenza, come previsto dalla disciplina dell'illecito aquiliano.

Ponendo la regola circa l'hosting provider (art. 14 § 3), la Direttiva menziona la possibilità per gli Stati membri di definire procedure per la rimozione delle informazioni o la disabilitazione: probabilmente aveva in mente la procedura di notice and takedown del diritto statunitense. Ne segue che questa, qualora venga istituita a livello nazionale, è liberamente regolabile dallo Stato, non essendo oggetto di armonizzazione, dal momento che la Direttiva stessa rinvia in modo esplicito la competenza nazionale e senza obbligatorietà[269]. La precisazione è utile, perché avrebbe potuto invece essere intesa come materia strumentalmente necessaria a creare armonizzazione sulla disciplina della responsabilità: invece la Direttiva chiarisce che esula dal proprio ambito applicativo e compete solo agli Stati, qualora vogliano istituirla (quindi compete loro sia nell'an sia nel quomodo). Potrebbe a dire il vero contestarsi ciò e sostenere –solo in astratto- che la procedura in questione fosse rilevante ai fini della creazione di un mercato unico ben funzionante per i

[267] Quest'ultima è la parte più signficativa del provvedimento. V. pure infra circa le inibitorie.

[268] Manna L., *La disciplina del commercio elettronico*, Cedam, 2005, 191, la quale però al tempo stesso scrive che la norma <<*non fa che ribadire l'irresponsabilità del provider per il caso in cui egli sia totalmente estraneo al contenuto dell'informazione, il che (..) non pare essere fonte di grossa novità nell'ambito del nostro ordinamento*>> (ma allora non si tratterebbe più di regola speciale!).

[269] Certa dottrina di lingua inglese erroneamente afferma l'obbligatorietà, parificando USA e UE: Bloch-Wehba H., *Automation in Moderation* (January 17, 2020), *Cornell International Law Journal*, Forthcoming, letto in ssrn.com, p. 11 del pdf).

servizi internet. Ad esempio la nuova Direttiva copyright impone agli Stati di adottare dei meccanismi di reclamo e ricorso, che però, dato il tenore della norma, par da intendere come meccanismi che operino ex post e cioè dopo che la rimozione o disabilitazione siano già avvenute. Ma così ha disposto il legislatore europeo. Tuttavia un'indicazione con rilevanza ex ante non manca e consiste nella necessità che la richiesta del titolare sia debitamente motivata. Il legislatore italiano, però, non ha colto questa possibilità per la dir. 2000/31, anche se potrebbe essere introdotta ora con una semplice modifica al d. lgs. 70/2003, che imponesse un contraddittorio con l'utente, al quale venisse trasmessa l'istanza del sedicente titolare con concessione di un breve termine per repliche[270].

14. Il caching provider (art. 15 d. lgs. 70/2003)

Il secondo tipo di provider regolato è quello che conduce un'attività di memorizzazione temporanea cosiddetta caching. Il "Web caching è la caching di documenti web (pagine HTML, immagini, ecc.) per permettere di ridurre l'uso della banda e il tempo di accesso ad un sito web. Una web cache memorizza copie di documenti richiesti dagli utenti, successive richieste possono essere soddisfatte dalla cache se si presentano certe condizioni"[271]. Si capisce dunque perché questo tipo di memorizzazione automatica, intermedia e temporanea[272] non generi responsabilità, se effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari e a loro richiesta (articolo 15 c. 1 prima parte). La legge però aggiunge una serie di ulteriori condizioni per fruire dell'esenzione, alcune delle

[270] Un piccolo contraddittorio è previsto dall'art. 7 del *Regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica* dell'AGCM (Delibera n. 680/13/CONS del 12 dicembre 2013 e succ. mod.).

[271] Così la voce *Web caching*, in *Wikipedia.*

[272] Nella disciplina del mere conduit la memorizzazione ammessa è definita non "temporanea", come qui, ma "transitoria" (art. 14 c. 2 d. lgs. 70/2003): fatico però a trarne differenza disciplinari (la distinzione lessicale è tuttavia presente anche nella altre versioni linguistiche della dir. 2000/31 da me controllate). Sono stati ricondotti al caching i servizi di posta elettronica, di organizzazione di mailing list/newsgroup/chatlines e di registrazione di nomi di dominio (Menichino C., *Art. 14 del d. lgs. 70/2003*, in *Codice del consumo* a cura di Cuffaro, Giuffrè, 5 ed., 2019, 1497): tuttavia di solito questi servizi generano pure una copia permanente sui server del provider (si pensi alle mail gestite via web anziché "in locale"), il quale allora diverrà un hosting provider.

quali non sono di immediata comprensione[273].

La prima (lett. a) è la più semplice da interpretare e consiste nel non dover modificare le informazioni stesse: la modifica pare da riferire al contenuto trasmesso (v. cons. 43 dir)[274].

La condizione sub b) sembra da intendere nel senso che non deve modificare o violare le condizioni di accesso ai dati presenti nella fonte originaria (la conformità dunque è rispetto alla fonte originaria): e cioè nel senso di non eludere restrizioni o di non modificare altri dati relativi all'accesso (come ad es. la sua localizzazione e cioè che non faccia apparire una URL diversa da quella vera[275]). In realtà la norma ha ampia portata, per cui fa perdere il safe harbour qualunque modifica della disciplina di accesso ai dati presente nella fonte.

Probabilmente fa perdere il safe harbour anche il mero violare un eventuale divieto di realizzare copie cache delle pagine di un sito (da vedere, allora, se basti un divieto espresso in linguaggio naturale oppure –come parrebbe- debba essere realizzato nel modo tecnologicamente adeguato per essere colto in automatico dai crawlers dei motori di ricerca)[276].

---

[273] La disciplina statunitense sulle condizioni di esenzione è assai più dettagliata: v. § 512 US Code, *Limitations on liability relating to material online*, sub (b) *System caching*, (2) *Conditions.* Taluno scrive che il safe harbour per gli hosting provider, ospitanti UGC (user generated content) riflette una presunzione di liceità dei materiali ospitati (Senftleben M., *The original sin. Content moderation (censorship) in the EU*, GRUR International, 2020/4, 339): l'affermazione non è condivisibile dato che la normativa si limita ad esentare il provider, senza nulla dire sulla liceità dei materiali, e semplciemetne lascia l'iniziativa al titolare dei diritti da questi eventualmente lesi.

[274] Da interpretare restrittivamente per Riordan J., *The liability of internet intermediaries*, cit., 399, § 12.104

[275] Così Bocchini R., *La responsabilità civile degli intermediari del commercio elettronico*, cit., 141; De Cata M., *La responsabilità civile dell'internet service provider*, Giuffrè, 2010, 196. Così pare Riordan J., *The liability of internet intermediaries*, cit., 400, § 12.105 (ma l'a. si riferisce a tutte e le prime tre lettere, come trasposte in UK).

[276] Questa opinione potrebbe trovarsi un appoggio nella giurisprudenza europea in tema di comunicazione al pubblico, in particolare nel caso *Land Nordrhein-Westfalen c. Renckhoff*, C.G. 07.08.2018, C-161/17. Secondo tale sentenza, il pubblico, considerato da chi mette on line una propria opera dell'ingegno, è solo quello del sito in cui l'ha caricata, anche in assenza di misure di protezione: a maggior ragione va rispettata la volontà del titolare quando non sia ipotetica ma esplicita, come nel caso ipotizzato nel testo. Che nella sentenza citata si tratti di giudizio sulla violazione o meno del diritto d'autore, mentre qui sulla invocabilità o meno del safe harbour, non fa particolare differenza.

le condizioni sub c) e sub e) hanno a che fare con il rapporto tra i dati memorizzati in cache e i dati originari e più precisamente l'aggiornamento dei primi rispetto ai secondi. La lettera sub c) impone l'onere di conformarsi ad eventuali standard di aggiornamento, che possono essere ritenuti "ampiamente riconosciuti e utilizzati dalle imprese del settore"[277]. Si tratta insomma –soprattutto per la lett. c)- di un classico esempio di clausola generale e in particolare di diligenza professionale, la quale curiosamente bypassa la definizione breve e va a concretizzarsi direttamente nel rinvio alle fonti esterne, secondo quanto aveva già colto Mengoni nella sua definizione del concetto di clausola generale. In breve, è come se la legge avesse imposto direttamente un obbligo di diligenza relativamente all'aggiornamento.

Altri[278] fa riferimento alla necessità di non trattenere le informazioni in cache per troppo tempo, dato che le pagine web sono oggetto di modifiche frequenti, sicchè la loro visione non aggiornata sarebbe di danno allo stesso provider. Il primo punto pare persuasivo, dato che la frequenza di svuotamento della cache incide sull'aggiornamento richiesto dalla lett. c). Il secondo punto lo è meno: la ragione dell'onere non sta nella

[277] E' stato sollevato il dubbio se l'espressione "indicate in modo ampiamente riconosciuto e utilizzato dalle imprese del settore" sia riferita alle informazioni oppure alle norme di loro aggiornamento: ed anzi questo a. opta per la prima alternativa, sulla base del dettato della legge delega (Manna L., *La disciplina del commercio elettronico*, Cedam, 2005, 195/6). Mi pare invece esatta la seconda alternativa, sia per la costruzione sintattica sia perché ha poco senso per la memorizzazione caching (anzi in generale) riferire gli standard di settore direttamente ai contneuti invece che alle modalità del loro aggiornamento, se si tiene conto che il dovere del caching è quello dell'aggiornamento/sincrnozizzazione rispetto al sito originario.. Nel diritto USA si v.la condizione di cui l'US code cit., al § 512.(b).(2).(B): <<*the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available*>>. Sulle prime, potrebbe opinarsi diversamente oggi in relazione al delisting chiesto ai motori di ricerca (qualicabili come caching provider) in base al diritto all'oblio: ma così non è, dato che il delisting è chiesto esercitando tale diritto soggettivo verso il titolare di uno specifico trattamento dati, il che nulla ha a che fare con le condizioni per fruire del safe harbour, che devono essere verificate in generale nel business sub iudice.

[278] Bocchini R.,, *La responsabilità civile degli intermediari del commercio elettronico*, cit., 141

tutela dell'interesse del provider, il quale baderà a sé stesso esercitando la libertà di impresa, quanto piuttosto nella tutela del pubblico dei navigatori: ed anzi sta nella tutela dei titolari delle situazioni giuridiche coinvolte nell'informazioni de quibus circa il loro diritto di controllare la diffusione quali-quantitativa dei dati che li riguardano. Quindi il dire che risulta determinante il fattore tempo, nel senso che, se la memorizzazione da temporanea diventa duratura, scatta la disciplina dell'hosting[279], è inesatto: la memorizzazione può essere duratura e rimanere tipologicamente caching, ma deve i) essere sottoposta ad aggiornamento ex lett. c) art. 15 d. lgs. 70/2003; e poi ii) essere appunto solo una cache cioè "specchio" di quanto memorizzato in un sito di origine.

La lett. e), dicevamo, riguarda sempre la questione dell'aggiornamento delle informazioni memorizzate in cache: solo che -a differenza dalla lettera c), che opera ex ante- qui il provider interviene ex post. Ex post nel senso che deve prontamente rimuovere le informazioni o disabilitare l'accesso, appena venuto a conoscenza del fatto che queste sono state rimosse nella loro sede originaria o che è stato disabilitato l'accesso alle medesime (a qualunque titolo: conta il dato oggettivo della sopravvenuta assenza in quel luogo, a prescindere da una correttamente formatasi volontà sottostante tali azioni, come invece i termini "rimozione" e "disabilitazione" potrebbero far pensare) oppure che la rimozione o disabilitazione sono state disposte da un giudice o da un'autorità amministrativa (sembra di capire che lo questo ordine dell'autorità giudiziaria o amministrativa riguardi la sede originaria, non il provider stesso, perché in tal caso è lecito presumere che il legislatore si sarebbe espresso in modo diverso[280]). In tal modo si dovrebbe ad es. evitare che la lesione, già arrecata, venga perpetuata[281].

[279] Bocchini R.,, *La responsabilità civile degli intermediari del commercio elettronico*, cit., 144.

[280] Ed inoltre tale ipotesi sarebbe in tutto o in parte già regolata dal c. 2 sull'inibitoria. Basta che vi stato l'ordine del'autorità, non essendo necessario che sia stato eseguito, come invece pare dire Manna L., *La disciplina del commercio elettronico*, cit., 198.

[281] Così Riccio G.M, *La responsabilità civile degli internet providers*, Giappichelli, 2002, 205 (ivi si legge "perpetrata" invece che "perpetuata": ma immagino sia frutto di una svista).

In sintesi le due lettere c) ed e) riguardano l'aggiornamento e la "coerenziazione" tra la fonte e la memorizzazione in cache: la lettera c) impone di farlo in via preventiva secondo gli standard di settore, mentre la lettera e) lo impone ex post cioè dopo aver ricevuto notizia della modifica nella fonte originaria. Ampliando la sintesi, le lett. b-c-e- riguardano tutte il rapporto tra memorizzazione cache e memorizzazione nella fonte originaria: la prima relativamente alle condizioni di accesso, le altre relative ai contenuti.

Da ultimo, la lettera d), quella dal significato meno chiaro, pare riferirsi alla possibilità che il provider setti la memorizzazione cache in modo da interferire nel (cioè ostacolare il) funzionamento di tecnologia (programmi) che i titolari dei diritti, coinvolti nelle informazioni, possano utilizzare per controllare la diffusione quali-quantitativa delle informazioni stesse[282]. La disposizione non precisa chi è il soggetto che può aver interesse ad avvalersi di soluzioni tecnologiche per raccogliere dati <<sull'impiego delle informazioni>>: ma parrebbe logico ritenere che fosse il titolare delle informazioni stesse o meglio il titolare del diritto ivi

[282] Così sostanzialmente anche De Cata M., *La responsabilità civile dell'internet service provider*, cit., 196/7 che scrive anche di una altra possibilità interpretativa consistente nel riferimentoi alla protezione di opera dell'ingegno digitali, concetto non molto chiaro. Similmente Manna L., *La disciplina del commercio elettronico*, cit., 196/7, se ben capisco, che riferisce l'interesse tutelato al "destinatario del servizio": espressione però equivoca poiché potrebbe far pensare all'utente del provider, anziché al soggetto leso dalla publicazione dei dati sulla rete, come a me pare, il quale non è affatto destinatario di alcun servizio da parte del provider (anche se i due ruoli coincidessero, quando il soggetto leso fosse causalmente cliente del provider, ciò sarebbe in linea teorica irrilevante, tranne specifiche pattuizioni ad hoc). V Sanna F, *Il regime di responsabilità dei providers*, cit., 289 ss. L'informazione sullo sfruttamento delle proprie opere è importante per decidere le modalità di licensing: v. l'accento posto dalla C.G. affinchè possa ravvisarsi consenso implicito: " *38 ogni autore deve essere effettivamente informato della futura utilizzazione della sua opera da parte di un terzo e degli strumenti di cui dispone per vietarla se intende farlo. 39. Infatti, in assenza di previa informazione effettiva quanto a tale futura utilizzazione, l'autore non è in grado di prendere posizione in proposito e, pertanto, di vietare, eventualmente, l'utilizzazione stessa, sicché l'esistenza stessa del suo consenso implicito al riguardo resta puramente ipotetica. 40 Conseguentemente, in assenza di garanzie che tutelino l'informazione effettiva degli autori quanto all'uso preso in considerazione delle loro opere e agli strumenti messi a loro disposizione per vietarlo, de facto è loro impossibile l'adozione di una qualsivoglia presa di posizione quanto a tale utilizzazione.*" (C.G. 16.11.2016, C-301/15, Soulier-Doke).

rappresentato o espresso. Se così è, immagino che il riferimento implicito sia soprattutto ai titolari di diritti di P.I. o simili, che tengano sotto controllo la diffusione delle loro creazioni o segni distintivi. Anche qui c'è un riferimento agli standard di settore, ma in senso diverso (opposto, verrebbe da dire) rispetto alla lett. c): in quest'ultima, come visto, il riferimento è all'onere gravante sul provider, di rispettare gli standard di aggiornamento e coerenziazione; nella lett. d), invece, il riferimento è agli standard utilizzabili dai titolari dei diritti, con i quali non deve interferire la memorizzazione cache praticata dal provider.

Infine al c. 2 è disposta la possibilità di inibitoria, come poi nell'art. 16 c. 3 e nel precedente art. 15 c. 23, cui rinvio. Secondo un a. la disposizione sarebbe non necessaria, dato che è prevista nel cons. 45[283]: ma incomprensibilmente, dato che da un lato il recepimento è obbligatorio, trattandosi di direttiva e non di regolamento e, dall'altro, che il considerando non ha efficacia vincolante.

15. Cenni sul contenzioso intorno a queste prime figure di provider

Queste prime due figure di provider hanno generato poco contenzioso[284]. Va però accennata la lite RTI c. Yahoo che ha riguardato il caching provider. RTI citò in giudizio Yahoo per violazione dell'inibitoria emanata da Trib. MI 09.09.2011 n. 10893-RG 79619/2009 e in subordine per violazione ("originaria" potremmo dire, non "derivata" dall'inibitoria) dei diritti di RTI. Il Trib. Milano con sentenza 25.09.2014 n. 11295-RG 19226/2012 respinge la domanda rilevando che nella sentenza del 2011 il comando era riferito alla sezione Video del portale Yahoo, mentre le violazioni ora portate in giudizio riguardavano il motore di ricerca Yahoo Italia Search. A parte ciò, entrando nel merito, il Tribunale ha ritenuto che la funzione di motore di ricerca, consistente nell'offerta di link correlati alla richiesta dell'utente, va inquadrato come cache provider, in quanto neutrale rispetto ai dati provvisoriamente memorizzati (§ 3). Ha aggiungo che la stessa conclusione vale per i connessi servizi di embedding (riproduzione sul sito Yahoo di immagini

[283] Riordan J., *The liability of internet intermediaries*, cit., 400, § 12.109.

[284] Per M. Husovec, *Injunctions aganist intermediaries*, cit., invece, sono significativi non solo l'hosting ma anche il *mere conduit* provider (p. 52)

collocate nel sito d'origine) e di suggest search (§ 4). Circa il linking e il suggest search, il giudizio è condivisibile: non c'è nemmeno la riproduzione o comunicazione al pubblico. Circa l'embedding, il giudizio appare invece più dubbio, dato che non pare rientrare nel concetto di <<*memorizzazione … effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta*>> ex art. 15. Sarà anche vero che è totalmente automatizzata (p. 23), ma non rispetta il predetto requisito. Il Trib. dice che il frame del sito di origine, presente sul portale Yahoo, è conseguenza di una scelta non di quest'ultimo ma del primo (p. 23). Se effettivamente Yahoo non potesse assolutamente evitare ciò, allora la cosa forse cambierebbe: forse, però, visto che anche in questo caso non si rispetterebbe il requisito indicato, che attiene al funzionamento tecnico-informatico del servizio. Ma pare dubbio che non possa impedire la riproduzione di queste immagini[285].

La Cassazione, adita ex art. 348 ter c.p.c. a seguito della dichiarazione di inammissibilità dell'appello, ha confermato l'esattezza della sentenza di primo grado, pur se senza approfondimenti degni di rilievo[286]: ha confermato, da un lato, l'esattezza della qualificazione del motore di ricerca come caching provider e, dall'altro, ciò che la legge dice chiaramente e cioè che il provider non ha alcun dovere di rimozione/disabilitazione prima dell'ordine dell'autorità[287].

Una decisione romana, ravvisando la qualità di mere conduit

[285] Il Trib. così sintetizza la irreponsaiblità del provider e l'assenza di nu obbligo ge4nerale di obbligo generale di sorveglianza o ricerca ex art. 17 c. 1 d. lgs. 70: <<*Come osservato dalla dottrina, tale irresponsabilità del prestatore del servizio rispetto alle informazioni memorizzate (in condizioni di neutralità rispetto ad esse) è stata il frutto della scelta del legislatore comunitario che ha assegnato l'onere di vigilanza sul rispetto dei diritti nell'ambito della rete telematica agli stessi titolari dei diritti stessi, non già agli internet provider. Ciò corrisponde all'esigenza di evitare sia di scoraggiare l'investimento e l'innovazione degli operatori della rete, che eventuali pregiudizi alla libertà di espressione in rete o la compromissione dei diritti degli utenti della rete quanto alla tutela dei loro dati personali e del diritto alla tutela delle loro comunicazioni (v. in particolare Corte di Giustizia UE, sentenza 24.11.2011, causa C-70/10, quanto all'impossibilità di imporre agli ISP sistemi automatici di filtraggio delle comunicazioni elettroniche anche in relazione a violazioni del diritto d'autore)*>> (§ 5)..

[286] Cass. 7709 del 19.03.2019 (a differenza della altra sentenza di pari data e tra le stesse parti, la n. 7708, in cui ci sono invece diversi spunti interessanti).

[287] P. 7 e risp. p. 10.

in Telecom, ha affermato che l'unica violazione concerneva il mancato avviso ex art. 17 c.3 d. lgs. 70/2003, per cui il suo titolo di responsabilità era diverso da quelli degli utenti/uploader. Per questo Telecom non poteva essere destinataria di provvedimenti repressivi della violazione da costoro commessa, dal momento che, non essendo costoro presenti in causa, non era possibile procedere ad accertamento della violazione da loro compiuta. Né in senso contrario si potrebbe opporre né l'inibitoria ex art. 14, c.2, che spetterebbe solo al giudice che accerta la violazione primaria né l'inibitoria ex art. 163 l. aut., che in nulla amplierebbe il raggio d'azione dell'inibitoria ex d. lgs. 70/2003[288]. L'interessante iussum cautelare richiederebbe maggior esame, sostanziale e processuale (anche sul fatto che la corresponsabilità ex art. 2055 c.c. di solito dà luogo a litisconsorzio facoltativo anziché necessario), per cui qui mi limito ad una breve osservazione. La sua apparente logicità potrebbe essere scalfita dal fatto che, anche si trattasse di hosting provider ex art. 16 d. lgs. 70/2003, la sua soggezione ad inibitoria ex c. 3 prescinde dal titolo di responsabilità e cioè esiste pure se egli non sia corresponsabile: è sufficiente che egli sia l'host del materiale illecito. Per cui processualmente potrebbe ravvisarsi nell'inibitoria ex c.3 un'azione in cessazione soggettivamente autonoma, sganciata dall'accertamento verso i titolari del fatto illecito. Analogamente potrebbe ragionarsi per il caso di mere conduit: il fatto che il titolo di responsabilità sia diverso da quello degli utenti, non dovrebbe impedire un accertamento della condotta degli utenti stessi limitato al solo ruolo di intermediario, finalizzato ad ottenere l'inibitoria. Tale accertamento, da un lato, sarebbe concettualmente diverso da quello costituito dalla violazione dell'art. 17 c.3[289] e, dall'altro, sarebbe naturalmente inopponibile agli utenti, uploader del materiale illecito.

In tema di search engines, è stato acutamente rilevato che la C.G. in *GC ed altri c. Google*, C-136/17, 24.09.2019, ai §§ 45-47, insegnando come applicare gli artt. 8 §§ 1 e 5 della dir.

[288] Trib. Rroma ord.15.04.2010, *FAPAV c. Telecom ed altri*, AIDA, XIX-2010, *1382*, pp. 1005-1006,.

[289] Anche se la diversità è minore di quanto si possa pensare (forse inesistente). Infatti la regola dell'art. 17 c.3 mira proprio ad evitare il protarsi della violazione primaria: per cui la sua violazione, in presenza di nesso di causalità, sarà probabilmente concausa del danno prodotto dalla diffusione del materiale illecito.

1995/46 o gli artt. 9 § 1 e art. 10 del reg. 2016/679 c.d. GDPR, ha esplicitamente costruito uno safe harbour per detti motori, così costruendo di fatto uno speciale regime di notice and take down all'interno dell'art. 9 GDPR[290] (riprendendo uno spunto delle Conclusioni dell'Avvocato Generale)[291]. Il passaggio è il seguente: <<*Pertanto, tenuto conto delle responsabilità, competenze e possibilità del gestore di un motore di ricerca in quanto responsabile del trattamento effettuato nell'ambito dell'attività di tale motore di ricerca, i divieti e le restrizioni [di cui agli artt. appena citt.] possono applicarsi (…) a tale gestore solo a causa di tale indicizzazione e, quindi, per il tramite di una verifica da effettuare, sotto il controllo delle autorità nazionali competenti, sulla base di una richiesta presentata dalla persona interessata*>>. Il punto è importante (meriterebbe specifico esame). A prima vista sembrerebbe trattarsi di un safe harbour speciale o meglio autonomo da quello della dir. 2000/31, dato che la Corte non la menziona: per cui pare trattarsi di un'applicazione diretta del canone della diligenza, esigibile da un internet service provider. Ricorre poi una significativa differenza, rappresentata dal fatto che l'illiceità è qui costituita non da materiali altrui, bensì dalla condotta stessa del motore di ricerca (la sua indicizzazione del dato altrui)[292].

Ricordo solo -data la scarsa chiarezza delle condizioni per fruire del Safe Harbor dell'articolo 15 (art. 13 dir. 2000/31)- l'interpretazione o meglio un esempio fornito da Cass. 7709/2019 circa la lettera B (<<si conformi alle condizioni di accesso delle informazioni>>). Secondo la Corte un esempio si ha quando il caching provider <<ometta di rendere disponibili al pubblico nella memoria cache delle informazioni che invece non sono tali nel sito di provenienza>> (p. 8, sub §3.1): dovrebbe però esserci un errore, dal momento che la norma pare voler dire che si fruisce dell'esenzione, quando le informazioni o il loro accesso nella memoria cache siano conformi a quanto è presente sul sito originario. In breve la coerenziazione tra

[290] Così acutamente Globocnik J., *The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17)*, in *GRUR International*, Vol. 69/4, April 2020, Pages 380–388, a 382-383, in https://doi.org/10.1093/grurint/ikaa002.

[291] Conclusioni AG Szpunar del 10.01.2019, C-136/17, alla prima questione, sub B, spt. § 56 (espressamente richiamato dalla C.G.).

[292] Profilo evidenziato da Globocnik J., *The Right to Be Forgotten*, op. loc. cit.

memorizzazione cache e quella nel sito originario dovrebbe portare a leggere l'inciso della cit. S.C. come se dicesse <<Omette di rendere disponibili al pubblico nella memoria cache informazioni che invece sono tali nel sito di provenienza>> oppure <<rende disponibili al pubblico nella memoria cache informazioni che invece non sono tali nel sito di provenienza>>. Se così fosse, però, l'interpretazione non parrebbe persuasiva, dal momento che, parlando di condizioni di accesso, la legge pare riferirsi proprio non ai contenuti, ma alla possibilità completa o ristretta di accedervi: l'esempio della S.C. si attaglia. invece. alla lettera c) oppure alla lett. e)[293].

Sempre di Cass. 7709/2019 va ricordato il principio di diritto, pure di dubbia esattezza, secondo cui <<nell'ambito dei servizi della società dell'informazione, la responsabilità del cd. caching, prevista dall'art. 15 del d.lgs. n. 70 del 2003, sussiste in capo al prestatore dei servizi che non abbia provveduto alla immediata rimozione dei contenuti illeciti, pur essendogli ciò stato intimato dall'ordine proveniente da un'autorità amministrativa o giurisdizionale>> (§ 3.1, in fine).

Infatti, da un lato, può essere fuorviante menzionare solo l'ordine dell'autorità, quando invece l'articolo 15 lettera e) menziona anche altri casi. Dall'altro lato, ricorre il (frequente, invero) errore, secondo cui il non rispettare le condizioni poste dall'articolo 15 c. 1 (come dall' articolo 16 c. 1 e dall'articolo 14 c. 1) comporta automaticamente l'affermazione di responsabilità. Al contrario, trattandosi di esenzione, il loro mancato rispetto comporta semplicemente la perdita della stessa, dovendosi poi giudicare secondo le norme comuni (anche se è probabile come si è detto sopra, che la condotta sia negligente e dunque si arrivi ad un'affermazione di illiceità appunto secondo dette norme comuni).

Da ultimo, questa Cassazione ribadisce al § 3.2 che al caching provider non è richiesto, anche quando sa di contenuti illeciti tramite diffida stragiudiziale o domanda giudiziale, di rimuoverli spontaneamente. Ciò è corretto, perché nell'art. 15

[293] Circa la lett. e), la SC parla di obbligo di cancellazione una volta che i dati siano rimossi dal sito originario o sia stato disabilitato l'accesso "ad opera del titolare" (§3.1). Quest'ultimo requisito non è posto dalla legge: sarà vero che di solito sarà il titolare ad effettuare questa operazione, ma ciò non rileva: il safe harbour opera se c'è una coerenza oggettiva tra le due memorizzaizoni, a prescidnere da ogni limitazione soggettiva circa il chi operi sul sito originario.

non c'è una norma come quella di cui all'articolo 16 c. 1 lett. B, che "obbliga" (meglio: onera) alla rimozione/disabilitazione appena notiziato. L'unica norma, che comporta un dovere per il caching provider di attivarsi, è allora l'articolo 17 comma 2, ove però il dovere consiste solamente nell'informare le autorità ed eventualmente fornire le informazioni indicative sul proprio utente[294].

16. L'hosting provider (art. 16 d. lgs. 70/2003). Esatta attuazione delle norme europee?

Veniamo infine all'articolo 16 che regola il terzo tipo di provider, cosiddetto hosting provider, dato che è colui che memorizza in via permanente i dati caricati dall'utente. Si tratta della fattispecie più frequente e comunque quella, sulla quale si son sviluppati massimamente il contenzioso e l'attività interpretativa della dottrina. E' proprio così che vengono a realizzarsi le attività lesive più disturbanti: sono infatti le piattaforme, ospitanti contenuti in via permanente destinati alla pubblica visione, a possedere maggiore maggior potenzialità lesiva.

L'incipit è lo stesso dell'articolo 14 e 15. Si dice che il provider non è responsabile qualora ricorrano le condizioni poi elencate. Non è chiaro se le due condizioni (lett. a e lett. b) siano poste in via alternativa ovvero congiuntiva: il tenore di quello nazionale parrebbe legarle invece tramite una congiuntiva a differenza dalle disposizioni della dir..

La normativa comunitaria con la disgiuntiva sembra porre due condizioni diverse in base a due specifiche situazioni (cioè una per ciascuna situazione), a seconda che il provider sia o meno a conoscenza della illiceità dei materiali ("dell'attività o dell'informazione") oppure[295] -nel caso di azioni risarcitorie- sia o meno a conoscenza di fatti che comunque rendano manifesta

[294] Fatto salvo quanto si osserva in questo scritto circa l'incostituzionalità delle disposizioni nazionali sul punto.

[295] Il dettato letterale (anche nella dir.) prevede una congiuntiva tra le due sottoipotesi della letta. a). Sarebbe forse meglio una disgiuntiva, dato che esse regolano il tipo di azione esercitata: risarcitoria o non risarcitoria. A meno che vengano esercitate entrambe nello stesso processo, nel qual caso la congiunzione sarebbe corretta. Resta però da capire quale sia –sempre che esista- l'azione civile diversa da quella risarcitoria, cui riferire la prima parte della lett. a): non l'inibitoria, che parrebbe regolata per intero dal seguente c. 3.

tale illiceità (cioè sempre dell'attività o dell'informazione)[296]. Nel caso (e fino a che) "non sia effettivamente a conoscenza" di ciò, il provider fruisce dell'esimente. Nel caso invece in cui ne sia a conoscenza, il provider è esentato solo se, appena venuto a conoscenza di tali fatti[297], agisce immediatamente per rimuovere i contenuti e/o disabilitare l'accesso. In breve, la costruzione dovrebbe allora essere la seguente: il provider non è responsabile i) se non sa; oppure ii) se sa, purchè, appena venuto a sapere, rimuova i contenuti e/o disabiliti l'accesso.

In generale, la trasposizione nazionale presenta due principali problemi interpretativi, riguardanti l'uno il rapporto tra la lett. a) e la lett. b) e, l'altro, la sola lett. b). Tuttavia qui li distinguo solo per comodità espositiva, dato che la soluzione dell'uno influenza quella dell'altro e dunque l'interpretazione deve procedere contestualmente. L'interpretazione è complessa, anche perché bisogna tener conto pure di quanto dispone l'art. 17, soprattutto il suo c. 3.

Quanto al primo problema, non dicendo nulla, la legge per alcuni sottintende[298] una congiuntiva tra la lett. a) e la lett. b) (necessità di entrambi i requisiti: tesi cumulativa) anziché una disgiuntiva (sufficienza di uno solo: tesi disgiuntiva). La tesi parrebbe da respingere almeno per tre motivi: uno di logica e gli altri di interpretazione complessiva, che tiene conto pure del secondo problema interpretativo dell'art. 17. Quanto al primo motivo, la tesi della congiunzione si baserebbe su

[296] Letteralmente "illegalità", ma è un errore, dovendosi leggere il medesimo termine già usato e cioè "illiceità" come prova il fatto che nel testo inglese è usato due volte il medesimo termine "illegal activity or information" e in tedesco "rechtswidrigen Tätigkeit oder Information".

[297] Letteralmente i "fatti" richiamati dalla lett. b) son solo quelli che la lett.a) seconda parte riferisce alle azioni risarcitorie, dato che la prima parte della lett. a) parla solo di "essere al corrente dell'illiceità", senza menzione di "fatti". Ma è ragionevole pensare che i fatti della lett. b) comprendano tutte e due le ipotesi della lett. a, come dimostra il testo inglese che più esattametne, dopo aver detto "*(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent*", alla lett. (b) dice "*the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information*". Del resto un diverso trattamento delle due azioni parrebbe privo di spiegazione.

[298] Solo "pare", però, non necessariamente: anche sotto il profilo meramente linguistico, infatti, potrebbe sostenersi una lettura reciprocamente disgiuntiva delle lettere a) e b).

un'interpretazione illogica, se non erro. Infatti si avrebbe che, per fruire del safe harbour, il provider dovrebbe trovarsi contemporaneamente nello stato soggettivo di non conoscenza (lett. a) e di conoscenza dell'illiceità (lett. b): il che non è possibile, potendosi chiedere o l'uno o l'altro, ma non entrambi. Si potrebbe obiettare che l'illogicità non esiste, dato che la lett. b) per il caso di conoscenza opera in un momento successivo a quello della lett. a) e cioè opera proprio quando il provider sia stato notiziato. Questo però non infirma il ragionamento, in quanto conferma invece che i due requisiti sono alternativi e cioè non possono operare nella medesima fattispecie concreta (conoscenza/non conoscenza). Per cui è più esatta la disgiuntiva europea, la quale potrà essere inserita nel testo italiano in via interpretativo-correttiva.

Quanto al secondo motivo per respingerla, la tesi congiuntiva oblitera la valenza precettiva della lett. a), se non erro. Infatti pretendere in ogni caso la comunicazione dell'autorità (lett. b), comporta che per ciò solo il provider sia sempre a conoscenza dell'illiceità dei file: la comunicazione infatti sarà motivata proprio in questo senso. Quindi la lett. a) perderebbe rilevanza e ciò in pratica equivarrebbe alla sua abrogazione. Il che non pare ammissibile, se esistono altre vie interpretative.

Il terzo motivo per respingerla è dato dal fatto che la legge delega, pur essendo muta sul punto (al pari dell'art. 16 d. lgs. 70/2003), intendeva però "dare organica attuazione alla direttiva 2000/31/CE": per cui può dirsi che vada interpretata come la dir. stessa e quindi con la disgiuntiva.

In senso contrario e cioè sfavorevole alla tesi disgiuntiva, diversi autori osservano che non pretendere un ordine dell'autorità renderebbe il provider arbitro del conflitto tra l'interesse del soggetto leso e quello dell'utente/cliente/uploader. Il che, tenuto conto della probabile inclinazione a privilegiare il primo, comporterebbe il rischio di lesione del secondo, soprattutto circa l'esercizio del libertà di manifestazione del pensiero. L'obiezione è seria ma, tutto pesato, pare preferibile rimanere con la tesi disgiuntiva. Rimando alle osservazioni sul punto esposte poco sotto.

Il secondo problema, di più difficile soluzione e vero punto di divergenza tra la norma nazionale (art. 16 c.1 lett. b) e quella europea (art. 14 c.11 lett. b), riguarda la necessità di comunicazione dell'autorità, richiesta dalla prima ma non dalla

seconda. Abbiamo appena visto infatti che l'esenzione italiana, nel caso che il provider sappia dell'illiceità, spetta solo se provveda ad immediata rimozione/disabilitazione "su comunicazione dell'autorità, competenti": cioè, parrebbe, la conoscenza, che fa scattare l'onere di rimozione/disabilitazione, è solo quella "qualificata", in quanto proveniente da un'Autorità. Il punto è' qui solo anticipato per chiarezza, ma verrà ripreso poi.

17. Esenzione da cosa?

Torniamo alla lett. a) la quale pure non è di cristallina chiarezza, pur se senza differenze rispetto alla dir. Qui varia la qualità della conoscenza richiesta a seconda che si tratti di azioni giudiziarie non risarcitorie (art. 16 c. 1 lett. a) prima parte) oppure risarcitorie ((art. 16 c. 1 lett. a) seconda parte). Nel primo caso deve trattarsi di conoscenza effettiva della illiceità dell'attività o delle informazioni, mentre nel secondo caso basta che sia al corrente di fatti, che rendano manifesta dette illiceità e cioè che questa sia percepibile in modo indiretto ma chiaro.

Non è difficile capire perché simile disposizione sia stata oggetto di diverse interpretazioni.

Si è detto da alcuni –è forse la tesi più diffusa- che la prima parte concerne la responsabilità penale e la seconda quella civile[299]. In senso contrario è stata rilevata la sua incongruità perché l'elemento soggettivo per la pretesa responsabilità penale ("conoscenza effettiva dell'illiceità") sarebbe meno accentuato di quello per la pretesa responsabilità civile ("illiceità manifesta"): sul presupposto che il primo sia appunto un quid

[299] Riccio G.M, *La responsabilità civile degli internet providers*, cit., 206; L. Manna, *La disciplina del commercio elettronico*, Cedam, 2005, 202/4. Quest'ultimo a. spiega ciò col fatto che nel penale, a differenza dal civile, l'imputato non va indenne da colpa "quando non intelligat quon omnes intellegunt", in quanto serve il diverso elemento soggettivo proprio di tale disciplina e col fatto che la effettiva conoscenza costituirebbe favoreggiamento personale: dimenticando però che la fattispecie astratta di questo reato prevede la punibilità di chi <<*aiuta taluno a eludere le investigazioni dell'autorità, comprese quelle svolte da organi della Corte penale internazionale, o a sottrarsi alle ricerche effettuate dai medesimi soggetti*>> (art. 378 c.p.) e che, tranne diversa disposizione, la punibilità richiede il dolo (art. 42 c.2 c.p.), difficilmente ravvisabili nella ordinaria condotta di un internet provider per il solo fatto che sia a conoscenza della illiceità. Tesi seguita da Montagnani M.L., *Internet, contenuti illeciti*, cit., 95.

minus rispetto al secondo, intendendo cioè la prima espressione (per la responsabilità penale) come sufficienza di una illiceità "anche solo dubbia", ed intendendo la seconda espressione (per la responsabilità civile) come necessità di una illiceità manifesta cioè conclamata[300]. La critica non pare calzante, dato che il secondo requisito pare invece più attenuato: si riferisce non alla consapevolezza della illiceità delle informazioni/attività non diretta ma solo indiretta e cioè relativa a fatti da cui discenda (pur se pianamente) l'illiceità delle informazioni/attività medesime. In altre parole, la norma pare negare il safe harbour, se il provider ha conoscenza diretta dell'illiceità delle informazioni ospitate (perché ad es. gli sono state portate a conoscenza dichiarazioni espresse o addirittura è compartecipe anche se magari defilato[301]) oppure se ce l'ha indiretta, quando l'oggetto della conoscenza è costituito da fatti altamente sintomatici dell'illiceità stessa[302]. Ecco allora ristabilita la maggior gravità di intento soggettivo per la presunta responsabilità penale e minore per quella civile[303]. In pratica la prima chiede un dolo per illecito di compartecipazione all'illecito dell'utente[304] mentre per la seconda basta la mera negligenza/colpa[305].

Secondo altri la lett. a) disciplinerebbe solo la responsabilità civile e le sue due regole si riferirebbero l'una al dolo

[300] De Cata M., *La responsabilità civile dell'internet service provider*, cit., 203, condividendo l'opinione di Minotti.

[301] Quest'ultima ipotesi della compartecipazione, infatti, impedisce di fruire del safe harbour proprio in base alla norma in esame.

[302] Potrebbe esserci un crescendo di situazioni intermedie tra l'essere compartecipe/concorrente, da un parte, e l'essere del tutto estraneo in assenza di ogni indice sintomatico dell'illiceità, dall'altra. Possono cioè ipotizzarsi situazioni in cui alla fine diventa sottilisimo il distinguo tra l'essere compartecipe nella modalità più lasca e l'avere conoscenza sì' indiretta ma tramiti ndici altametne sintomatici.

[303] Analogamente Sanna P., *Il regime di responsabilità dei providers intermediari*, cit., 291.

[304] Difficilmente infatti in tale caso il provider, oltre a perdere il safe harbour, eviterà l'affermazione di responsabilità concorsuale in base alla disciplina generale.

[305] Così infatti intendono alcuni, che ravvisano menzionata nella norma solo la responsabilità civile: Nivarra L:, voce *Responsabilità del provider*, Dig. disc. civ., Utet, 2003, p. 1195. Anche qui tale negligenza farà perdere il safe harbour e determnerà la probabile affermazione di responsabilità concorsuale in base alla disciplina generale

(consapevolezza dell'antigiuridicità) e l'altra alla colpa (consapevolezza dell'esistenza di materiali sospetti)[306].

La disposizione però non precisa alcunché e dunque pare preferibile ravvisarvi l'esenzione da responsabilità non solo civile. Anche se di fatto sarà quasi sempre quella penale, lascerei aperta la possibilità a qualunque altra responsabilità, ad es. amministrativa[307]. Anzi l'intenderei nel modo più ampio e cioè come esenzione da qualunque conseguenza giuridica sfavorevole[308]. Questo pare infatti l'approdo più sensato di una normativa sovranazionale, che ha voluto trovare un compromesso tra gli Stati membri su un attività (quella del provider) che costituiva un mezzo di assai più rapida diffusione, rispetto al passato, sia di materiali illeciti che di informazioni e idee lecite: e che dunque preannunciava potenzialità enormi. Pertanto, per proteggere questa industria nascente (quindi forse anche per competere adeguatamente con gli Stati Uniti), detto compromesso è stato trovato, da un lato, nell'individuare un'area, entro cui gli operatori avessero la certezza di essere esente da ogni conseguenza pregiudizievole, e, dall'altro, nell'esplicitare che non erano gravati da un dovere generale di controllo[309]. Si è giustamente osservato che <<il quadro

[306] così forse Nivarra L., voce *Responsabilità del provider,* cit., 1198.

[307] Conf. le conclusioni 16.03.2016 dell'A.G. Szpunar in *Mc Fadden contro Sony*, C-484/14: <<*Come risulta dai lavori preparatori del citato atto normativo, la limitazione in esame copre, in modo orizzontale, ogni forma di responsabilità per attività illecite di ogni natura. Si tratta dunque della responsabilità tanto penale o amministrativa quanto civile e della responsabilità tanto diretta quanto secondaria, per gli atti commessi da terzi*>> (§ 64). Analogamente le conclusioni dell'§AG Saugmandsgaard ØE in C.G., C-682/18 e C-683/18, *Peterson c. Google-Youtube e Eelsevier c. Cyando*, § 138.

[308] Conf, su questa portata per tutti gli safe harbour della dir. M. Husovec, *Injunctions aganist intermediaries*, cit., 58.

[309] Disposizione quest'ultima che potrebbe parere a tutta prima inutile, dato che il safe harbour dipende dalal consapevolezza di fatti specifici, non generici. Ma inutile in realtà non è, dato che, come più volte osservato in questo scritto, il safe harbour è appunto un'esenzione da responsabilità (quindi dispone in negativo), mentre eventuali obblighi dic ontrollo generalizzati sarebbero fonte di responsabilità (quindi la disposizione vieta simili disposizioni positive di responsabilità). La normativa ha voluto <<*approntare un primo livello di armonizzazione delle normative nazionali degli Stati membri su « taluni aspetti » della società dell'informazione, con un'impostazione che nasce ab origine priva del carattere di completezza e di organicità dal punto di vista sistematico, ma che mira a soddisfare primordiali esigenze di normazione*>> (Bravo F., voce *Commercio elettronico*, cit., § 24, 306)..

normativo di riferimento considera dunque, in linea di principio, gli Isp come meri intermediari e come tali non sottoposti alla disciplina dettata dagli art. 15 e 21 Cost. per i fornitori di contenuti>>[310].

Lo spirito dunque della disciplina posta dall'art. 16 c.1 sembra essere che l'esenzione c'è, fino a che il provider non sappia nulla (purché non sia colposamente ignorante: probabilmente l'illiceità manifesta va intesa come necessità di una colpa grave) oppure, qualora sappia, se ha subito rimosso/disabilitato. C'è però una discrepanza non piccola tra il testo comunitario e il testo nazionale (secondo problema interpretativo, sopra anticipato), la quale complica l'interpretazione.

La discrepanza sta nel fatto che mentre la lettera a) è quasi uguale[311], nella lettera B la norma nazionale inserisce il requisito della comunicazione da parte dell'autorità: <<non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso>>.

La disposizione nazionale non è ben scritta e risulta di difficile interpretazione. Non è chiaro se la comunicazione delle autorità sia riferita alla conoscenza dei fatti (cioè come se fosse: "non appena a conoscenza di tali fatti per aver ricevuto comunicazione delle autorità competenti") oppure all'azione di rimozione o disabilitazione (come se fosse: "non appena a conoscenza di tali fatti, ed essendogli stato comunicata la necessità di rimozione da parte delle autorità competenti, agisca immediatamente…"). Nel primo caso non dovrebbe però esserci la virgola tra il primo periodo il secondo della lettera b); nel secondo caso, più che comunicazione, dovrebbe essere stato usato il termine "richiesta" oppure "ordine". In ogni caso rispetto al testo europeo c'è un requisito in più, che è quello della necessità di un qualche intervento da parte dell'autorità[312]. Come anticipato, questo requisito nemmeno è menzionato tra i criteri

[310] Così Donati F., *Internet (diritto costituzionale)*, Enc. dir., Annali, VII, 2014, § 6.

[311] C'è qualche piccola ma direi irrilevante variazione, ad esempio "al corrente" è sostituito con "a conoscenza" e "illegalità" è sostituito con "iliceità".

[312] Qualunque delle due possibili soluzioni indicate nel testo si scelga, infatti, non dovrebbe esserci dubbio che la norma nazionale subordina il sorgere del dovere di rimozione/disabilitazione al ricevimento della comunicazione da parte dell'autorità.

direttivi della delega, i quali riproponevano tale e quale la corrispondente norma della dir.[313]. Visto che la delega è uguale alla direttiva e dunque non ci sono problemi di incompatibilità tra le due, non c'è il conseguente rischio di disapplicazione della prima da parte del giudice[314]. Il problema è a valle ed è un problema di coerenza del decreto delegato con la legge delega. L'inserimento del requisito della comunicazione da parte dell'autorità costituisce una scostamento non irrilevante dalla delega[315]: con la conseguenza che questa norma o questa porzione di norma parrebbe incostituzionale (v. infra) e ciò per entrambe le possibilità interpretative accennate.

Addirittura pare essere incongrua la disciplina delle due lettere a) e b), se lette disgiuntamente[316]. Secondo la lett. a), il safe harbour c'è fino a che non sa, il che significa che, se sa, risponde civilmente: a meno che –va aggiunto- provveda a rimuovere i contenuti e/o disabilitare l'accesso. Questa limitazione è ovvia e va aggiunta dato che non si può dire che il provider non è esentato se sa e poi non permettergli di liberarsi dalla responsabilità facendo l'unica cosa che è in suo potere: il

[313] Legge 1 marzo 2002 n. 39 Art. 31 c.1 lettera f) n. 3.

[314] Se invece già la legge delega contenesse principi e criteri direttivi incompatibili con la dir. allora andrebbe disapplicata: con conseguente disapplicabilità a valle ("per derivazione") pure del d. delgato che desse fedele attuazione alla delega. Quid iuris in tal caso se poi il d. delegato si discostasse dalla delega per restare fedele alla dir.? Sarebbe viziato da incostituzionalità per eccesso di delega, vien da dire: il parametro di costituzionalità dell'atto delegato è solo la delega, visto che il governo non ha potere legislativo autonomo. Nel caso de quo fornalmente il parametro è dato solamente dalla legge delega, dato che questa i principi e criteri direttivi li ha posti, sicchè non si può dire che ricorra il caso di delega tramite rinvio ai principi presenti nella dir. stessa (Ruotolo M.-Spuntarelli S., Art. 76, *Comm. alla Cost.* a cura di Bifulco R.-Celotto A.-Olivetti M., Utet giuridica, 2006, II, 1500). Resta il fatto che li prende tali e quali dalla dir., praticamente senza alcuna elaborazione nazionale (ricorre quindi lo stesso la "parziale abdicazione del Parlamento al compito di determinarli" evidenziata dalla dottrina: Iannuccilli L. (a cura di), *L'evoluzione politipica" della delega legislativa*, § 6, in *La delega legislativa, Seminario di studio* (prob. 2008), leggibile in *www.cortecostituzionbale.it*).

[315] E quindi anche dalla direttiva, il che però è irrilevante, dato che il confronto va fatto con la legge delega. Diverso sarebbe stato se fosse la legge delega a contrastare la dir.

[316] Se interepretate come congiuntamente necessarie, la lett. a) perderebbe di senso, essendo già contenuta nella lett. b): infatti la conoscenza di per sé non basterebe, servendo l'ordine dell'Autorità (conf. De Cata M., *La responsabilità civile dell'internet service provider*, cit., p.201)

venire a conoscenza spesso non dipende da lui, per cui gli si deve dare la possibilità di liberarsene e lo può fare solo tramite rimozione/disabilitazione (ed entro tempi brevissimi). Secondo la lett. b) –a parte la difficoltà interpretativa sopra indicata-, l'invocabilità del safe harbour la si perde se, ricevuta la comunicazione o la richiesta dell'Autorità, non si provveda anche qui alla rimozione/disabilitazione. Ma allora la necessità della comunicazione autoritativa pare diventare inutile, dato che, anche se manca ma il provider pur sempre sa dell'illiceità, alla luce della lett . a) può mantenere il safe harbour solo se provvede subito a fare la stessa cosa (rimozione/disabilitazione). Questo presuppone un rapporto disgiuntivo tra lett. a) e lett. b). Si potrebbe opporre che tra le due lettere corresse invece un rapporto congiuntivo e cioè che dovessero operare assieme: ma allora diventerebbe inutile la lett. a), dato che, per quanto egli sappia, dovrebbe attendere l'ordine dell'Autorità per l'obbligo/onere di rimuovere.

In breve, salvo errore, se i due requisiti son letti come congiuntamente necessari, è inutile la lett. a); se son letti come disgiuntamente necessari, diventa superfluo l'ordine dell'Autorità di cui alla lett. b)

18. L'hosting provider può attendere fino al ricevimento di un ordine dell'autorità senza perdere il safe harbour?

Approfondiamo il punto. Come anticipato, qualche dottrina ha sostenuto la necessità di attendere l'ordine dell'Autorità, per non mettere il provider nello scomodo ruolo di arbitro della liceità dei materiali, con rischio per qualunque scelta faccia: se accogliere l'istanza del soggetto sedicente leso (col rischio di violare il contratto con l'utente uploader) o se rigettarla, esponendosi però al rischio di azione giudiziaria da parte del medesimo[317]. La tesi si basa su un'esigenza molto seria ma, alla fine, non pare condivisibile.

Infatti la necessità di un ordine dell'Autorità è esclusa sia dalla legge delega sia dalla Direttiva: che sia esclusa, lo si ricava dal fatto che entrambe non lo menzionano per l'hosting

[317] Così diversi aa., ad es.: Tescaro M., *Una proposta ricostruttiva contrastante con il diritto vivente in tema di responsabilità civile dell'internet provider*, cit., 73 ss.; Bravo F., voce *Commercio elettronico*, cit., 311-312; sostanzialmente pure L. Manna, *La disciplina del commercio elettronico*, cit., 205-207.

provider[318], mentre, quando hanno voluto richiederlo, lo hanno fatto espressamente[319]. La tesi qui sostenuta è seguita dalla giurisprudenza europea[320] e dal noto precedente Trib. Napoli Nord 3 novembre 2016[321].

Allora la disciplina nazionale, in sintesi (tenuto conto pure dell'art. 17 c. 2), potrebbe essere ricostruita così: - se il provider nulla sa, non risponde (art. 16 c.1 lett. a) ; ii) se sa, non è tenuto

[318] Art. 31 c.1 lett. f sub 3 per la legge delega n. 39 del 2002.

[319] Per la legge delega 39/2002 v. art. 31 c..1 lett. g) e lett. l). Ma v. anche ivi la lett. m) (art. 19 d. lgs. 70/2003) che prevede la possibilità di composizione stragiudiziale "in caso di dissenso" tra utente e provider: il che fa propoendere per la non necessità di ordine dell'Autorità, che elimina dubbi e dissensi, sostituendosi d' imperio alle opinioni delle parti in lite. Per la dir. v. il § 3 degli artt. 12, 13 e 14.

[320] In tale senso C.G. 12.07.2011, C-324/09, *L'Oreal ed altri c. eBay ed altri*: <<*Inoltre, affinché non siano private del loro effetto utile, le norme enunciate all'art. 14, n. 1, lett. a), della direttiva 2000/31 devono essere interpretate nel senso che riguardano qualsiasi situazione nella quale il prestatore considerato viene ad essere, in qualunque modo, al corrente di tali fatti o circostanze*.>>, § 121, e C.G. 08.09.2016, C-160/15, *GE Media BV c. Sanoma ed altri*, § 49: <<*Per contro, qualora sia accertato che tale persona era al corrente, od era tenuta ad esserlo, del fatto che il collegamento ipertestuale da essa collocato forniva accesso a un'opera illegittimamente pubblicata su Internet, ad esempio perché ne era stata avvertita dai titolari del diritto d'autore, occorre rilevare che la messa a disposizione di detto collegamento costituisce una «comunicazione al pubblico»*>>. Indirettamente pure da C.G. 26.04.2017, C-27/15, *Stichting Brein c. Wullems*, § 49, laddove –circa il concetto di <<essere al corrente o essere tenuti ad esserlo>> del'illiceità, richiama i §§ 49-51 di GS Media. In senso contrario Tescaro M., *Una proposta ricostruttiva contrastante con il diritto vivente in tema di responsabilità civile dell'internet provider*, cit., 75/6, il quale, pur riconoscendo la contrarietà dell'opposta sua tesi (necessità di una comunicazione dell'autorità) al ragionamento della C.G., valorizza però il richiamo ivi contenuto alla diligenza dell'operatore economico. Tuttavia, da un lato, la normativa europea lascia intendere abbastanza chiaramente che non è necessario attendere alcuna comunicazione di pubbliche autorità e così pure la stessa sentenza *L'Oreal c. eBay* (anche laddove afferma che il giudice <deve tenere conto> della notizia di parte: altrimenti dovrebbe non tenerne conto alcuno); dall'altro, utilizzare il criterio della diligenza, con la conseguente possibilità di applicazioni diversificate a livello nazionale, rischierebbe di compromettere l'uniforme applicazione del diritto nella UE. Tuttavia la norma interna c'è, per cui, come si osserva nel testo, essa vige sino ad abrogazione o a sua dichiarazione di incostituzionalità.

[321] Pubblicata in varie riviste, tra cui *Giur. it*., 2017, 629 ss a p. 631, nota di Bocchini. Il giudice napoletano aggiunge anche il maggior danno per il soggetto leso procurato dall'attendere un ordine dell'Autorità rispetto al danno per l'utente/uploader procurato dalla rimozione/disabilitazione immediata (punti 4-5): questo però, varrà in casi eclatanti, come quello ivi sub iudice, ma pare assai difficile affermarlo in via generale.

a rimuovere i contenuti e/o disabilitare l'accesso fino a che non gli giunga un'ordine dell'Aut. (art. 16 c. 1 lett. b); -se sa ed anche senza alcun ordine dell'Aut., deve informare l'Autorità stessa (art. 7 c.2 lett. a)[322]; - a prescindere dal fatto che sappia o no, deve fornire le informazioni in suo possesso per identificare l'utente quando ne venga richiesto dall'Autorità.

E' vero che come sopra anticipato, la norma (art. 16 c. 1 lett. b)) pare affetta da vizio di incostituzionalità, laddove attribuisce rilevanza solo alla comunicazione dell'autorità, visto che: i) né la norma UE né la delega nazionale lo prevedono (l'incostituzionalità è naturalmente prodotta dal mancato rispetto di quest'ultima) in quanto dalla prima è desumibile la rilevanza della conoscenza comunque acquisita e tale è l'interpretazione della C.G.; ii) l'aggiunta nazionale modifica sensibilmente la composizione tra interessi confliggenti, posta da tale regola europea. Però, fino a che non venga dichiarata l'incostituzionalità, la norma vige: da noi, infatti, il giudizio di costituzionalità non è decentrato, ma accentrato presso il Giudice delle leggi[323]. Nemmeno pare possibile disapplicarla per

[322] Nell'art. 17 c.2 lett. a) il sapere è meno approfondito di quello indicato nell'art. 16 c.1 lett. a): in quest'ultima norma è chiesto una conoscenza effettiva dell'illiceità o di fatti che la rendano manifesta, nella prima invece basta la conoscenza di "presunte attività illecite", meglio da riformulare in "attività presuntivamente illecite".

[323] Il che conferma la non condivisibilità dell'applicazione diretta e diffusa delle norme costituzionali da parte del singolo giudice, come propone certa dottrina (Perlingieri e la sua scuola: ad es. Perlingieri P., *Interpretazione e controllo di conformità alla Costituzione*, in *Rass. dir. civ.*, 2018/2, 593 ss, ad es. § 7; Perlingieri P., *<<Controllo>> e <<conformazione>> degli atti di autonomia negoziale*, in Rass. dir. civ., 2017/1, 204 ss, § 7; Perlingieri G., *Portqlis e i <<miti>< della certezza del diritto e della c.d. <<crisi>> della fattispecie*, Ed. sc. ital., 2018, ad es. p. 44 ss, p. 51 ss e 71/2). Potranno esserci dei casi, in cui è chiara la prevalenza di un interesse su quello antagonista, ma in molti altri non sarà così. Per evitare dunque le gravi incertezze cui darebbe luogo il giudizio diffuso di costituzionalità, pare preferibile quello accentrato: in base ad esso, allora, l'applicazione diretta delle norme costoitzuionali da parte del singolo giudice è ammessa solo entro limiti ristretti (soprattutto intepretazione adeguatrice e clausole generali). Sul tema v. ad es. i molti scritti di D'Amico G., tra cui *Applicazione diretta dei principi costituzionali e integrazione del contratto*, in *Giust. civ.*, 2015/2, 247 ss e *Problemi (e limiti) dell'applicazione diretta dei principi costituzionali nei rapporti di diritto privato (in particolare nei rapporti contrattuali)*, in *Giust. civ*., 2016/3, 443 ss. Resta però qualche dubbio. ad es. può capitare che in casi gravissimi attendere la dichiarazione di incostituzionalità per dare l'adeguata tutela possa produrre medio tempore danni irreparabili –magari ledendo beni giuridici primari- al titolare del diritto leso. In situaizoni simili

difformità dalla direttiva, stante l'inapplicabilità diretta di quest'ultima nei rapporti tra privati[324]: l'orientamento, nonostante qualche "sbandata", pare essere fermo[325], dato che vanificherebbe la distinzione tra direttiva e regolamenti, molto chiara nel diritto costituzionale europeo.

Si potrebbe osservare che la possibilità per l'hosting provider, di attendere l'ordine dell'Autorità senza perdere il safe harbour, si appoggiasse alla norma sulla responsabilità civile posta dalla legge delega: col che verrebbe meno l'errore attuativo della delega, sopra visto. Secondo l'art. 31 c.1 lett. l), infatti, la legge delegata avrebbe dovuto attenersi al seguente criterio direttivo: "prevedere che il prestatore di servizi è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha usato la dovuta diligenza;". Potrebbe infatti dirsi (forse) che, come il risarcimento del danno spetta solo dopo l'inottemperanza ad ordine dell'Autorità, così fino al medesimo momento nessun onere di rimozione/disabilitazione incombe sul provider: con la conseguenza, per cui egli potrebbe mantenere i file denunciati senza perdere il safe harbour. In altre parole il

sarebbe eversivo il giudice che disapplicasse *singulatim* la norma di legge (a suo dire) incostituzionale?

[324] Si può eventualmente pensare ad una responsabilità dello Stato per scorretta attuazione dei comandi portati dalla dir. 2000/31. Il danno risarcibile allora sarebbe quello causato dalla esposizione online delle informazioni protrattasi tra il primo avviso e l'ordine pubblico di rimozione/disabilitazione: è infatti presumibile che, se la norma europea fosse stata recepita correttamente (sufficienza della notizia dei file illeciti comunque ricevuta), il provider avrebbe proceduto alla rimozione/disabilitazione già dalla richiesta del soggetto leso..

[325] La dottrina specialistica ricorda alcune sentenze della C.G. che distinguono tra effetti diretti orizzontali, non riconosciuti, e obbligo per i giudici di disapplicare le norme interne difformi, invece riconosciuto (Strozzi G.-Mastroianni R., *Diritto dell'Unione Europea. Parte istituzionale*, Giappichelli, 2019, 8 ed., 313 ss.). La tesi parrebbe però poco persuasiva. Per lo più, infatti, non ci sarà differenza pratica tra riconoscere diritti ai privati in base alla dir. non (o mal) attuata, da una parte, e disapplicare le norme interne a ciò ostative: in entrambi i casi la decisione si fonderà sulle situazioni soggettive riconosciute dalla dir. Qualche differenza potrebbe darsi nell'attività stragiudiziale, in cui ancora non interviene il dovere disapplicativo del giudice. Ma se le parti non concordano, allora si va in giudizio e la differenza viene meno.

requisito della comunicazione dell'Autorità, previsto dall'art. 16 c.1 lett. b d. lgs. 70/2003, avrebbe base giuridica nella cit. norma della legge delega.

Tuttavia non pare che le cose stiano così. Da un lato, questa norma della legge delega è stata attuata da altra norma del d. lgs. 70/2003 e cioè dall'art. 17 c.3. Dall'altro, la norma stessa riguarda solo il risarcimento del danno e cioè la responsabilità risarcitoria, mentre sulla disciplina del safe harbour (l'esenzione da responsabilità) la delega è uguale alla dir. Quindi, sotto il profilo formale, rimarrebbe la distonia tra delega e legge delegata in tema di safe harbour. Si è infatti sopra tenuto distinto il profilo –negativo- dell'esenzione da responsabilità (safe harbour) da quello –positivo- dell'ascrizione di responsabilità.

Potrebbe però replicarsi che, pur vero ciò sotto il profilo formale, nella sostanza comminare la responsabilità solo dopo l'inottemperanza ad ordine dell'Autorità finisce per influenzare anche l'individuazione del momento a partir da quale decorre l'onere di procedere a rimozione/disabilitazione[326]. Ciò potrebbe parere sensato, in termini di politica legislativa astratta. Però, data la vigente convivenza di due ordinamenti giuridici (europeo e nazionale)[327] e dato che il primo si limita a regolare l'esenzione da responsabilità e non l'affermazione della stessa (una norma come l'art. 17 c.3 non esiste nella dir.), va accettato che il vincolo europeo concerna solo l'esenzione: ed allora la distinzione va mantenuta. Ne segue allora che il provider, se ottempera già alla diffida stragiudiziale, fruisce appieno del safe harbour e la cosa finisce li. Il problema invece sorge se egli sceglie di disattendere la diffida di parte e attendere l'ordine dell'Autorità per la rimozione/disabilitazione, basandosi: i) o sulla tesi interpretativa cumulativa dell'art. 16 c.1 lett. a-b; ii) oppure, anche nell'ottica della tesi disgiuntiva, sul fatto che alla

[326] In altre parole in un'ottica complessiva parrebbe illogico distinguere l'esenzione da responsabilità dalla sua ascrizione positiva, creando un'area (concettualmente) intermedia di dubbio.

[327] E' noto che invece la C.G. insiste nella tesi monistica, probabilmente perché quella dualistica rende più precario o meno capace di espansione l'ordinamento europeo: il quale (o i cui effetti) risulterebbe giustificato solo nei limiti in cui gli Stati espressamente vi hanno acconsentito. Sul punto ha fatto scalpore la sentenza della Corte Costituzionale tedesca 5 maggio 2020 che ha allentato il vincolo di partecipazione della Bundesbank al PSPP Public Sector Purchase Programme della BCE.

peggio perderà sì il safe harbour –profilo negativo-[328], consapevole però che la principale misura a suo carico (risarcimento del danno) –profilo positivo- non potrà scattare, atteso che l'art. 17 c.3 è inequivoco nel prevedere che ciò avvenga solo dopo l'inottemperanza all'ordine dell'Autorità[329].

Se così è, però (e nell'ottica della tesi disgiuntiva[330]), può sorgere il dubbio che la disciplina risarcitoria ex art 17 c. 3 prima parte d. lgs. 70/2003 sia incompatibile con la direttiva stessa: precisamente col suo safe harbour che, come più volte detto, è riconosciuto solo se la rimozione/disabilitazione avviene subito dopo la diffida stragiudiziale[331]. E' vero che il legislatore ben può arricchire quella europea, dato che come noto <<la direttiva vincola lo Stato membro cui è rivolta per quanto riguarda il risultato da raggiungere, salva restando la competenza degli organi nazionali in merito alla forma e ai mezzi.>> (art. 288 c.2 Tratta. UE). Bisogna però che la legge nazionale sia compatibile con la piena attuazione della direttiva. Il dubbio sollevato va però probabilmente respinto, in quanto la cit. disposizione nazionale non osta alla piena applicazione di quella europea. Che lo Stato ricolleghi la (positiva) responsabilità per inottemperanza alla diffida stragiudiziale oppure all'ordine dell'Autorità, è indifferente per il comando europeo: a questo interessa solo che già dopo la richiesta di parte, se c'è pronta ottemperanza, operi il safe harbour. In altre parole, anche se la prassi sarà nel senso che i provider per lo più attenderanno l'ordine dell'Autorità per rimuovere o disabilitare, colui, che invece scegliesse di provvedervi sin dalla diffida stragiudiziale, fruirebbe in pieno del safe harbour: con piena attuazione della

[328] Sempre che il giudice non sollevi questione di costituzionalità dell'art. 16 c.1 lett. b), come sopra ricordato.

[329] E' del resto abbastanza chiaro che la disposizione, per cui il provider <<e' civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorita' giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente etc.>> (art. 17 c.2), va intesa nel senso che è responsabile solo a partire da tale momento e giammai prima.

[330] I provider italiani opteranno verosmilmente per attendere l'ordine dell'autorità, stante il dettato normativo nazionale e fino a che non si diffonda un orientamento giurisprudenziale diverso. Ma potrebbero anche optare per rimozione/disabilitazione ante iussum iudicis per motivi reputaizonali.

[331] Se valga solo quella del titolare del diritto leso oppure anche la notizia proviente da terzi, è altra questione interessante. Probabilmente è esatta la seconda, se ben circostanziata.

dir.[332].

19. Posizione di garanzia? Primo arbitro tra interessi in conflitto, da dirimere tramite congruo bilanciamento

Taluno parla di <posizione di garanzia> dell'internet provider[333], ma non pare opportuno, non corrispondendo all'usuale concetto di "posizione di garanzia". Quest'ultima, semmai, è propria dell'editore, non dell'intermediario digitale: la legge anzi vuol evitare proprio un simile status, rendendo l'internet provider responsabile solo quando sa "con ragionevole sicurezza" della presenza di materiali illeciti. Del resto parlare di garanzia per la situazione successiva all'ordine dell'autorità pare poco esatto, trattandosi solo di adempimento di un ordine ad hoc. La posizione di garanzia, come viene normalmente intesa, è ben più pregnante, essendo fonte di obblighi anche prima di ordini ad hoc dell'autorità e per il solo fatto di rivestire una certa carica connessa più o meno strettamente all'autore del fatto (come ad es. nella responsabilità dei "padroni" ex art. 2049 cc)[334]. In sostanza, col concetto di "posizione di garanzia" si indicano i casi, in cui si risponde del fatto altrui o comunque quando il titolare è dotato di potere decisionale che permette di prevenire violazioni[335]: mentre la responsabilità del provider per

[332] La dottrina ha evidenziato la maggior certezza offerta dalle due discipline statunitensi (§ 230 CDA e § 512 DMCA) rispetto a quella europea, ove si deve tener conto delle circostanze del caso (Petruso, R., *La responsabilità degli intermediari della rete telematica.*, cit., 76 ss, 157 a livello europeo e 175-6 a livello di applicazione giurisprudenziale nazionale, a dispetto del tenore che richeide una comuncazione dell'Autorità).

[333] Delfini, cit. da Manna L., *La disciplina del commercio elettronico*, cit., 206, nt 105. Contraria Allegri M.R., *Ubi social, ibi ius*, cit., 54.

[334] La funzione di garanzia, svolta dal predetto titolo di responsabilità, è affermata da Franzoni M., *Dei fatti illeciti. Art. 2043-2059*, cit., sub art. 2049, pp. 351-2.

[335] Corsaro L., voce *Responsabilità per fatto altrui*, *Dig. sez. civ.*, 1998, § 3, plurisonline. V.si soprauttto l'elaborazione penalistica sulla responsabilità degli organi di governo: ad es. Pedrazzi C., voce *Società commerciali (disciplina penale)*, in *Dig. penale*, 1997, Plurisonline, § 1.4: *<<I reati societari hanno natura propria, presupponendo nel soggetto attivo il possesso di determinate qualifiche; ciò che ovviamente non esclude che anche gli extranei possano risponderne a titolo di concorso(12). Le qualifiche più frequentemente ricorrenti (di amministratore, direttore generale, sindaco e liquidatore) si ricollegano a specifici ruoli funzionali definiti dalla normativa privatistica, corredati da un complesso di poteri e di obblighi rispetto al quale le ipotesi delittuose si connotano come abuso o violazione. Lo stretto legame tra responsabilità civili*

non aver ottemperato alla richiesta di rimozione (da chiunque provenga[336]) è responsabilità da fatto proprio. La disciplina complessivamente intesa, allora, pare all'opposto aver escluso per lui una responsabilità da posizione di garanzia ed averla invece ancorata solo alla propria omissione (omessa rimozione/disabilitazione).

Del resto il ruolo dell'internet provider di "primo arbitro"[337] tra interessi confliggenti (utente uploader vs. terzo riguardato dalla informazione caricata) è inevitabilmente sempre più frequente, dato che le comunicazioni umane sempre più si spostano su internet (per non dire che, rispetto alle violazioni commesse, i casi poi portati in sede giudiziale saranno pochissimi e per i soliti motivi: incertezza giuridica, costi, disparità di posizione socioeconomica)[338]. Si pensi al conflitto

verso la società e verso i terzi e responsabilità penali non consente di dubitare della derivazione privatistica delle categorie soggettive in questione. E soprattutto è la normativa privatistica cui ci si richiama per riconoscere nelle suddette figure altrettante «posizioni di garanzia» in funzione degli interessi penalmente tutelati: da cui l'obbligo dei soggetti in parola, nell'ambito delle rispettive competenze, di far uso dei poteri d'intervento loro conferiti dalla legge per impedire che le norme penali vengano violate da altri intranei>>. Oppure Centonze F., *Controlli societari e responsabilità penale*, Giuffrè, 2009: la posizione di garanzia è una "*categoria concettuale con la quale una consolidata elaborazione penalistica indica la cerchia dei poteri e dei doveri di agire a salvaguardia degli interessi tutelati e individua la sfera della responsabilità individuale: essere titolare di una posizione di garanzia vuol dire, nell'ottica dei reati omissivi, avere il dovere e il potere di attivare gli strumenti necessari a governare le fonti di rischio e a impedire il verificarsi di eventi pregiudizievoli per gli interessi tutelati*" (p. 122/3, corsivo nell'originale), precisando più avanti che "*L'ampiezza dei poteri giuridici ricavabili dalla normativa civilistica e di quelli concretamente esercitabili nella realtà aziendale segna Dunque in modo invalicabile la sfera dei doveri posti in capo ai singoli consiglieri non esecutivi: la determinazione delle posizioni di garanzia nelle organizzazioni complesse devi infatti ispirarsi al <<criterio fondamentale>> della <<corrispondenza fra poteri e doveri>> … Correlativamente i limiti del potere segnano, per ciascun obbligato, il limite invalicabile della garanzia esigibile*>> " (p. 164, citando una Relazione ad un progetto di riforma del cod. pen.; corsivo e virgolettato nell'originale).

[336] Conf. De Cata M., *La responsabilità civile dell'internet service provider*, cit., 202.

[337] Primo perché è il primo ad intervenire. Seguirà poi eventualmente un reclamo amministrativo (ad es. v. il regolamento AGCOM o la recente dir. copyright 790/2019 art. 17 § 9) e -ancora dopo- azione in corte.

[338] Sostanzialmente per questo motivo un a. scrive di <<*privatizzazione del potere giudiziario*>> e di *quasi-judicial role* con riferimento ai motori di ricerca (Haber E., *Privatization of the Judiciary* (February 20, 2016), 40 *Seattle U. L. Rev.*

tra diritto alla riservatezza e diritto di cronaca. Vale la pena di riportare il passo pertinente in cui la C.G. ha così concluso, valorizzando il ruolo del motore di ricerca (Google): << - *L'articolo 8, paragrafo 2, lettera e), della direttiva 95/46 deve essere interpretato nel senso che, in conformità di tale articolo, un gestore siffatto può rifiutarsi di accogliere una richiesta di deindicizzazione ove constati che i link controversi dirigono verso contenuti che includono dati personali rientranti nelle categorie particolari di cui all'articolo 8, paragrafo 1, ma il cui trattamento è incluso nell'eccezione di cui all'articolo 8, paragrafo 2, lettera e), sempre che tale trattamento risponda a tutte le altre condizioni di liceità poste dalla suddetta direttiva e salvo che la persona interessata abbia, in forza dell'articolo 14, primo comma, lettera a), della medesima direttiva, il diritto di opporsi a detto trattamento per motivi preminenti e legittimi, derivanti dalla sua situazione particolare. - Le disposizioni della direttiva 95/46 devono essere interpretate nel senso che il gestore di un motore di ricerca, quando riceve una richiesta di deindicizzazione riguardante un link (...) deve – sulla base di tutti gli elementi pertinenti della fattispecie e tenuto conto della gravità dell'ingerenza nei diritti fondamentali della persona interessata al rispetto della vita privata e alla protezione dei dati personali, sanciti dagli articoli 7 e 8 della Carta – verificare, alla luce dei motivi di interesse pubblico rilevante di cui all'articolo 8, paragrafo 4, della suddetta direttiva e nel rispetto delle condizioni previste in quest'ultima disposizione, se l'inserimento di detto link nell'elenco dei risultati, visualizzato in esito ad una ricerca effettuata a partire dal nome della persona in questione, si riveli strettamente necessario per proteggere la libertà di informazione degli utenti di Internet potenzialmente interessati ad avere accesso a tale pagina web mediante una ricerca siffatta, libertà che è sancita all'articolo*

115 (2016), passim, spt. sub II, pp. 129-139, leggibile in ssrn.com, soprattutto a seguito della sentenza 13.05.2014 della C.G. sul diritto alla deindicizzazione in *Google Spain*, C-131/12. L'a. esprime forti preoccupazioni e avanza alcune proposte di intervento (p. 160 ss). Sostanzialmente condivide Geddes K., *Meet Your New Overlords: How Digital Platforms Develop and Sustain Technofeudalism*, cit., p. 472/3 (anche se la critica trascura che la piattaforma è un'impresa privata, pur se divenuta –per sua forte scelta- risorsa essenziale: per cui il paragone tra la ademocraticità delle piattaforme e la democraticità del potere giudiziario statale è poco calzante). L'inevitabilità del ruolo quasi arbitrale è sottolineata da Soro A., *Democrazia e potere dei dati*, cit., 51-52.

11 della Carta>>[339]. Compito non certo semplice per il provider[340], tenuto poi conto delle diverse tradizioni giuridiche

[339] C.G. 24.09.2019, C-136/17, § 69, *GC, AF, BH, ED c. Commission nationale de l'informatique et des libertés (CNIL), int.: Primo Ministro e Google*.

[340] Per non dire del difficile bilanciamento tra: i) esigenza repressiva di hate speech, tesi negazioniste dell'Olocausto, fake news etc.; ii) esercizio della libertà di espressione; iii) necessità di fare profitti (come sopra ricordato, la moderazione dei contenuti è sopratutttto influenzata dalla *corporate philosophy*, dalla *regulatory compliance*, dalle proteste del pubblico e dall'esigenza di *profit maximization* secondo Sander B., *Freedom of Expression in the Age of Online Platforms*, cit., sub II.B, 948 ss.; l'a segnala una crescente attenzione delle piattaforme per la tutela dei diritti umani, ivi 963/4), alla luce poi del fatto che la moderazione "umana" è data in outsourcing ad aziende estere e soprattutto delle Filippine data la loro miglior conoscenza del modo di pensare statunitense (per le relazioni tra i due paesi) e soprattutto dati i bassi livelli retributivi (così, circa Facebook, Carmi E., *The Hidden Listeners: Regulating the Line from Telephone Operators to Content Moderators*, in *International Journal of Communication*, 2019, vol. 13, 448/9: sono i c.d. *commercial content moderators-CCMs*, tenuti nascosti da Facebook per le ragioni indicate dall'a.; invece in Germania la *content moderation* è delegata al gruppo Bertelsmann, come si legge in Kaye D., *The global struggle to govern the internet*, *Columbia global reports*, 2019, 59). Un panorama dettagliato sulle modalità pratiche di svolgimento della *content moderation*, con interviste anonime di moderatori statunitensi e filippini, in Roberts S. T., *Behind the screen. Content moderation in the shadows of social media*, Yale university press, 2019: lo scopo del libro (p. 3 e 201) è gettare luce su un mondo che i social media hanno da sempre tentato di tenere nascosto sia per le difficili condizioni di lavoro dei moderatori –anche sotto profilo psicologico a causa del materiale "pesante" che devono vagliare-, sia perché può incrinare pesantemente l'immagine di comunicazione diretta e non filtrata tra gli utenti, che i social hanno saputo creare: ad es. v. 24 ss., 38, 60 ss., 71, 111 ss., 170 ss sulle Filippine, 209 ss; v. a 41-43 una tassonomia dei rapporti di lavoro adottati per per questa poco conosciuta attività e a p. 140 ss l'interessante cenno dell'estensione d'attività di una di queste imprese, cui la *moderation* è data in outsourcing, al settore probabilmente più redditizio del *brand management*. Per l'a. la *human moderation* non è recessiva, nonostante il sempre più massiccio ricordo all'intelligenza artigficiale, ed anzi aumenterà: pp.207/209). E' stato suggerito che anche le piattaforme uniformino le loro regole all'art. 19 dell'*International Covenant on Civil and Political Rights* del 1966 (promosso dall'ONU) -in particolare circa i limiti al right to freedom of expression posti dal c. 2 (concetti un po' vaghi, per vero)-: così Aswad E. M., *The Future of Freedom of Expression Online*, 2018, *17 Duke L. & Tech. Rev. 26* (sub III, p. 57 ss, v. esame di vantaggi e svantaggi derivanti dall'adeguamento a tale disciplina e la conclusione che i primi prevarrebbe sui secondi). Le policies delle piattaforme <<*often display a fundamental tension between a corporate reluctance to intervene and "a fear of not intervening," with "a range of registers on display: fussy schoolteacher, stern parent, committed fellow artist, easygoing friend."*>> (Aswad E. M., *The Future of Freedom of Expression Online*, cit., 42, a sua volta citando Gillespie T., *Custodians of the internet*, cit., 48-50, ma del quale sul punto va letto l'intero cap. 3 *Community guidelines, or the sound of no* e, sulla complessità della *mderation*, p. 9 ss). Aswad ricorda (p. 39-40) che l'altro modo (oltre alle rispettive policies),

nazionali[341], per il quale la moderazione umana è inevitabile[342].

Arbitro, naturalmente, non solo nell'an ma anche nel quomodo delle misure necessarie per rimediare: si v. la nota decisione C.G. 24.09.2019, C-507/17, Google c. Commission nationale de l'informatique et des libertés (CNIL) e molti intervenuti[343]. Qui però le difficoltà per l'internet provider

---

con cui i social possono ledere la freedom of expression, consiste nella collaborazione con gli Stati che non rispettano i diritti umani (v. pure della stessa a. Aswad E. M., *In a World of "Fake News," What's a Social Media Platform to do?*,in *Utah Law Review*, Vol. 2020/4, passim ma spt. II.B-II.C, p. 1021 ss). Sul tema è abbastanza attiva l'UE: v. infra nota 404. Stante il ruolo di gatekeepers della comunicazione, la relazione tra Governi e piattaforme è complessa, variando da Stato a Stato, su cui v. ad es.: - Karanicolas, M., *Squaring the Circle Between Freedom of Expression and Platform Law*, Pittsburgh Journal of Technology Law & Polic, 2020, vol. XX 175.ss, sub I.B, 183-191, passim; - Gorwa R., *What is platform governance*, cit., p. 857 e p.861; Kaye D., *The global struggle to govern the internet*, cit., 27 ss. (l'a. è il referente ONU per il *right to freedom of opinion and expression*); - Keller D., *Who Do You Sue? State and Platform Hybrid Power over Online Speech, Hoover Institution, Aegis series paper n. 1902*, 2019, p. 5-7 (sulle pressioni esercitate dai governi, c.d. *jawboning*); - Klonick K., *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression* (June 30, 2020). Yale Law Journal, Vol. 129/8, 2439-2448, anche sulle interrogazioni parlamentari statunitensi e europee di Zucherberg; Bloch-Wehba H., *Global Platform Governance: Private Power in the Shadow of the State*, *72 SMU L. Rev.* 27 (2019), passim (ad es. 39, 43, 66), centrato proprio sul rapporto opaco tra grandi piattaforme e Stati. Non piccoli problemi linguistico-organizzativi ha Google per il tracciamento e la vendita degli spazi pubblicitari connessi al suo motore di ricerca, a seconda degli Stati (Bilic P., *Search algorithms, hidden labour and information control*, cit., p. 5). Le difficoltà per le piattaforme di conciliare la loro globalità con le specificità di ciascuna comunità statale sono bene esposte nel saggio di Bickert M., *Defining the boundaries of free speech on social media*, cit., passim (come detto sopra, è manager di Facebook) e in Klonick K., *The Facebook Oversight Board*, cit., 2474 ss, sull'impossibilità di applicare a tutti i paesi i medesimi Community Standards, alla base della *content moderation*.

[341] Circa il diritto all'oblio ad es. viene evidenziato il diverso approccio europeo (privilegiante la privacy o protezione dei dati personali) rispetto a quello statunitense (privilegiante il diritto di parola tramite la forte protezione offerta dal Primo Emendamento): Bloch-Wehba H., *Global Platform Governance: Private Power in the Shadow of the State*, *72 SMU L. Rev.* 27 (2019), p. 58/9

[342] V. approfonditamente Gillespie T., *Custodians of the internet*, cit., 111. Anzi, la moderazione dei contenuti è la vera *commodity* offerta dalle piattaforme (Gillespie T., *Custodians of the internet*, cit., p. 13, seguito da Douek E., *Verified Accountability*,in *Hoover Institution-Aegis series paper n. 1903*, p. 5-6).

[343] *<<È compito, inoltre, del gestore del motore di ricerca adottare, se necessario, misure sufficientemente efficaci per garantire una tutela effettiva dei diritti fondamentali della persona interessata. Tali misure devono soddisfare tutte le esigenze giuridiche e avere l'effetto di impedire agli utenti di Internet negli Stati*

paiono essere superabili: la Corte pare infatti riferirsi al suo dovere di deindicizzare in modo geograficamente selettivo (UE/extraUE, in linea di massina) con modalità tali da evitare che la decisione sia aggirabile con stratagemmi tecnici. Addirittura Amazon, per gestire le allegazioni di violazioni brevettuali sul suo marketplace e non perdere venditori importanti, ha creato una propria procedura di notice and take down, sulla falsariga di quelle giudiziali (da qui il nomignolo "District of Amazon Federal Court"), che attualmente dovrebbe essere ancora allo stato sperimentale[344].

Sempre su questo tema è ancora intervenuta nel 2019 la C.G. dicendo che l'eventuale inibitoria si estende ai contenuti equivalenti a quelli accertati illeciti, anche se il giudice deve precisare i confini di tale equivalenza in modo da non costringere il provider a difficili decisioni sul punto[345]. Si tratta

membri di avere accesso ai link in questione a partire da una ricerca effettuata sulla base del nome di tale persona o, perlomeno, di scoraggiare seriamente tali utenti(v., per analogia, sentenze del 27 marzo 2014, VUPC Telekabel Wien, C-314/12, EU:C:2014:192, punto 62 e del 15 settembre 2016, Mc Fadden, C-484/14, EU:C:2016:689, punto 96)>>, § 70 e poi anche § 73. E' la nota decisione sulle modalità di deindicizzazione - statale/europea/mondiale - da parte del motore di ricerca, quando un soggetto vi abbia diritto (deindicizzazione non coincide con oblio: differenze esposte in Scarpellino C., *Un oblio tutto europeo*, nota a C.G. 24.09.2019, C-507/17, cit., *Danno e resp*., 2020/2, 213-215).

[344] Come ipotizzabile però sconta dei difetti, primo dei quali il conflitto di interessi in capo ai decisori nominati naturalmente … proprio da Amazon (esame in Emerson K.Y., *From Amazon's domination of e-commerce to its foray into patent litigation: will Amazon succeed as "the District of Amazon Federal Court*"?, in *North Carolina journal of law§technology*, vol. 21/2, dic. 2019, p. 93 ss.).

[345] Vale la pena di riportare i passi pertinenti: *<<45 Tenuto conto di quanto precede, occorre che le informazioni equivalenti cui fa riferimento il punto 41 della presente sentenza contengano elementi specifici debitamente individuati dall'autore dell'ingiunzione, quali il nome della persona interessata dalla violazione precedentemente accertata, le circostanze in cui è stata accertata tale violazione nonché un contenuto equivalente a quello dichiarato illecito. Differenze nella formulazione di tale contenuto equivalente rispetto al contenuto dichiarato illecito non devono, ad ogni modo, essere tali da costringere il prestatore di servizi di hosting interessato ad effettuare una valutazione autonoma di tale contenuto [corsivo agg.]. 46 Ciò posto, un obbligo come quello descritto ai punti 41 e 45 della presente sentenza, da un lato, nella misura in cui si estende anche alle informazioni di contenuto equivalente, risulta sufficientemente efficace per garantire la tutela della persona oggetto di dichiarazioni diffamatorie. Dall'altro, tale tutela non viene garantita tramite un obbligo eccessivo imposto al prestatore di servizi di hosting, in quanto la sorveglianza e la ricerca che richiede sono limitate alle informazioni contenenti gli elementi specificati*

di un tentativo della C.G. di semplificare la vita al provider, che deve decidere se il successivo caricamento riguarda materiali equivalenti o meno a quelli già dichiarati illeciti. La precisazione del giudice sarà naturalmente sempre poco soddisfacente: se troppo ristretta, è facilmente aggirabile; se troppo ampia, genererà molti dubbi nel provider e di conseguenza contenzioso in fase applicativa, con opposizioni all'esecuzione quando sia assistita da penali o astreintes[346].

Sul punto si vedano pure le recenti sezioni unite sul conflitto tra diritto di cronaca e diritto all'oblio (Cass, sez. un. 22.07.2019 n. 19.681). Secondo tale pronuncia, la ripubblicazione "a distanza di un lungo periodo di tempo" di una notizia soddisfa un interesse storiografico (cioè alla rievocazione) e non più di cronaca, sicchè va eseguita in forma anonima[347], dato che "il trascorrere del tempo modifica l'esito del bilanciamento"[348]: a

nell'ingiunzione e il loro contenuto diffamatorio di natura equivalente non obbliga il prestatore di servizi di hosting ad effettuare una valutazione autonoma, e quest'ultimo può quindi ricorrere a tecniche e mezzi di ricerca automatizzati..>> (C.G. 03.10.2019, C-18/18, Eva Glawischnig-Piesczek c. Facebook, §§ 45-46) (v. pure infra). La sufficienza del ricorso alla tecnologia, così affermata, è contestata da Cavaliere P., *Glawischnig-Piesczek v Facebook on the Expanding Scope of Internet Service Providers' Monitoring Obligations* (December 1, 2019). (2019), *European Data Protection Law Review* 5(4):573 – 578, letto in ssrn.com, pp. 6/7.

[346] V. sotto per il cenno a questo problema classico dell'inibitoria.

[347] Ivi, § 9, il che è coerente con la minimizzazione del trattamenta disposta per tali casi dall'art. 89 reg. 679/2016 GDPR.

[348] Nel caso specifico, ventisette anni e si trattava di omicidio. Nel caso Google Spain (cit. infra) la C.G. ha deciso analogamente in una fattispecie in cui i fatti erano anteriori di doci anni rispetto all'stanza di cancellazione (gennaio e marzo 1998 - marzo 2010, § 14; anche se la Corte poi scrive di "16 anni prima", § 98). La C.G. precisa che nel bilanciamento non rileva il fatto il protrarsi del trattamento sia o meno fonte di pregiudizio (§ 96 e 99): profilo interessante, quasi fosse ammissibile qualunque scelta idiosincratica del titolare verso i trattamenti di questo tipo, al pari dei diritti dominicali. Forse sarebbe stato meglio precisare il punto, dato che si potrebbe sostenere che il protrarsi ingiustificato del trattamento cagiona sempre un pregiudizio, anche se non patrimonialmente valtuabile: altrimenti l'istanza di delisting non verrebbe avanzata. La differenza pratica tra le due impostazioni sorgerebbe, quando –ipotesi di scuola, probabilmente- il titolare del diritto leso, pur dichiarando o avendo aliunde dichiarato di non ravvisre alcun pregiudizio di alcun tipo per sé, ciò nonostante chiedesse la deindicizzazione. Probabilmente però è corretta la precisazione della C.G.: l'esercizio del diritto di decidere quali dati divulgare di sé e come divulgarli –in questo alla fine consiste la riservatezza- prescinde dalla ricorrenza di qualunque pregiudizio, anche non patrimoniale, e costituisce dunque un'esclusiva di tipo (strutturalmente) dominicale.

meno che "non sussista un rinnovato interesse pubblico ai fatti ovvero il protagonista abbia ricoperto o ricopra una funzione che lo renda pubblicamente noto"[349]. Il § 9 si conclude con la precisazione: "la materia in esame di per sé sfugge ad una precisa catalogazione e richiede di volta in volta, invece, la paziente e sofferta valutazione dei giudici di merito".

Ebbene, inevitabilmente tale valutazione attenta incomberà, prima della lite, all'editore, ma potrà porsi anche per il provider: anche quest'ultimo dovrà farla, quando richiesto di rimuovere o disabilitare materiali in violazione del diritto all'oblio (anziché dei diritti soliti all'onore o reputazione o di proprietà intellettuale). E non si tratta di valutazione facile, dato che la SC così sintetizza gli orientamenti europei: <<*il bilanciamento tra l'interesse del singolo ad essere dimenticato e quello opposto della collettività a mantenere viva la memoria di fatti a suo tempo legittimamente divulgati presuppone un complesso giudizio nel quale assumono rilievo decisivo la notorietà dell'interessato, il suo coinvolgimento nella vita pubblica, il contributo ad un dibattito di interesse generale, l'oggetto della notizia, la forma della pubblicazione ed il tempo trascorso dal momento in cui i fatti si sono effettivamente verificati*>> (§ 7, in fine)[350]. Si pensi solo alla valutazione: i) del quantum di tempo necessario per mutare la qualificazione da diritto di cronaca a diritto alla ricerca storiografica[351]; e/o ii) del quantum di

[349] Ed inoltre può essere talora utile o necessario addure i nomi, poiché questi "servono anche per dissociare la responsabilità degli onesti" (così giustamente A. Bonetta, *Diritto al segreto del disonore. "Navigazione a vista" affidata ai giudici merito*, in *Danno e resp*., 2019/5, 618, in nota a Cass. su.19681/2019. cit.)

[350] Si pensi poi all'applicazione delle regole poste dall'art. 17 *Diritto alla cancellazione (<<diritto al'oblio>>)* del reg. GDPR 679/2016. Il titolare del trattamento (l'intemediario esegue un trattamento: per Google Search lo afferma la prima sentenza europea sul diritto al''oblio Google c. AEPD-Gonzalez 13.05.2014, C-C-131/12, § 41) deve valutare se -a seguito di istanza di cancellazione- i dati personali "non sono più necessari rispetto alle finalità per le quali sono stat iraccolti o altrimetni trattati" (§ 1 lett.a) e soprattutto se ricorra l'esimente del- "*l'esercizio del diritto alla libertà di espressione e di informazione*" (§ 3, lett. a).

[351] Così pure, inevitabilmente, R. Pardolesi, *Oblio e anonimato storiografico: <<usque tandem …>>?* in nota alle s.u. 19681/2019, cit., *Il Foro it.*, 2019/10, sub III, che riferisce dell'opposta valutazione nel diritto tedesco e avanti la Corte Europea dei Diritti dell'Uomo nel caso M.L. e W.W. c. Repubblica federale di Germania ric. nn. 60798/10 e 65599/10, la quale è commentata da C. Morini, *Il bilanciamento tra diritto all'oblio, libertà di espressione e conservazione della memoria collettiva in una recente sentenza della Corte europea dei diritti*

rilevanza pubblica del soggetto; iii) del quantum di pubblicità dell'interesse pubblico alla diffusione[352]. La dottrina ha approfondito il modo, con cui un provider europeo dovrebbe affrontare correttamente una richiesta di notice and take down basata sul diritto all'oblio, modo che dà bene l'idea della complessità della valutazione lasciata al provider.[353]. Addirittura si dubita: -che nel diritto UE l'insegnamento, impartito dalla C.G. in Google Spain sul diritto all'oblio per i motori di ricerca, si applichi agli hosting providers e ai social[354]; - circa il modo con cui vada conciliato l'apparente conflitto tra disciplina sulla protezione dei dati e quella del safe harbour, alla luce delle disposizioni di reciproca salvezza (art. 2 § 4 reg. UE 2016/679; art. 1.5.b, dir. 2000/31)[355]. A riprova della complessità del

dell'uomo, in *MediaLaws. Riv. dir. media*, 3/2018). La cosa è ancora meno semplice, se si considera che per certi aa. il diritto all'oblio non è tutelato in sé, ma solo come mezzo per offrire un'aggiornata rappresetnazione di sé e cioè come modalità di esercizio del diritto all'identità personale (Bianca M., *Memoria ed oblio: due reali antagonisti?*, in *Riv. dir. media*, 2019/3, 29/30): per cui andrebbe vagliata sotto questo profilo l'intimazione del richeidente la cancellazione/anonimizzazione.

[352] Cass. s.u. 19681/2019, cit., § 9, in fine. La S.C. lascia però solo il giudice di merito in questo difficile giudizio, non fornendogli criteri di bilanciamento (ha perso un'occasione in tal senso, secondo Calabrese G., *Rievocazione storica e diritto all'oblio*, *Danno e resp*., 2019/5, 623/4).

[353] V. gli interessanti lavori di: Kuczerawy A.-Ausloos J., *From notice-and-takedown to notice-and-delist: implementing Google Spain*, in *Colorado tech. Law jour*., 2016, vol. 14/2, 219 ss, 247 ss <Appendix: Criteria For Delisting>; e di Keller D., *The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation*, in *Berk. tech. law jour.*, 2018, vol. 33, 327 ss., che indica otto step da seguire. La procedura, stante la quasi totale automazione sia delle notices che delle risposte delle piattaforme, produce pesanti e preoccupanti effetti di disincentivazione (*chilling effects*) della comunicazione online sulle piattaforme medesime (così, dati alla mano, Penney J., *Privacy and Legal Automation: The DMCA as a Case Study* (September 1, 2019), in *Stanford Technology Law Review*, Vol. 22, No. 1, 412 ss.: l'a. riferisce di due *case studies* condotti tramite sondaggi, p. 436 ss e risultati sub IV a 445 ss, e ne trae alcune implicazioni, sub V a 463 ss)

[354] Keller D., *The Right Tools: Europe's Intermediary Liability Laws*, 322 ss.

[355] Keller D., *The Right Tools: Europe's Intermediary Liability Laws*, cit., 351 ss.. Per questa a. va fatta prevalere la dir. 2000/31 per le questioni su materiali caricati dagli utenti, sicchè la procedura ex GDPR riguarderà solo le violazioni proprie del provider (cioè sui c.d. *back-end data*, id est quelli opachi all'utente come file di log o profilazioni), p. 351 ss, passim, e spt. 363-364 (la distinzione tra i due tipi di dati -*back-end data* e *online expressions*- percorre tutto il saggio). Direi comunque che, in base al principio *lex posterior derogat priori*, applicabile

bilanciamento, sono arrivate le linee guida dell'European Data Protection Board per i motori di ricerca[356].

Che un bilanciamento tra così rilevanti interessi sia affidato ad un ente privato con fine lucrativo, quale è un internet provider, può sorprendere e preoccupare[357]. Infatti queste imprese non hanno come obiettivo quello di rendere più sicure le comunicazioni on line oppure (quanto alla content moderation) quello di calibrare il bilanciamento tra la moderazione umana e quella algoritmica: piuttosto il loro scopo è <<*to hold and expand their dominion over networked information flows. They protect this position by, among other things, developing products that users cannot resist or acquiring*

pure al diritto UE, prevarrà il GDPR e dunque il safe harbour sarà sempre applicabile, qualunqe sia la violazione di *data protection* allegata.

[356] *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR* (part 1), del 7 luglio 2020.

[357] Si chiede se sia opportuna una sì ampia discrezionalità Astone M., Right to be forgotten online *e il discutibile ruolo dei gestori dei motori di ricerca*, nota a C.G. C-507/17 e a C-136/17, cit., *Diritto di nternet*, 2020/1, 32-33 (lasciando intendere una risposta negativa); contesta la nebulosità delle regole di bilanciamento imposte al motore di ricerca Orefice M., *Diritto alla deindicizzazione: dimensione digitale e sovranità territoriale (Corte di giustizia c-507/17)*, nota a C.G. 24.09.2019, C-507/17, Google c. CNIL, in *Rivista AIC*, 2020/1, spt. § 6. Addirittura si caldeggia un arretramento dell'intevento giudiziale, nel senso di liberarlo dalle questioni di merito sulle singole istanze all'hosting provider (ex post), per limitarlo alla equità della sua policy di content moderation (solo ex ante, dunque, se ben capisco): la moderazione, insomma, sarebbe lasciata in modo decetnralizzato agli utenti, i quali <<should be the filters>>, tipo Wikipedia (Hartmann I.A., *A new framework for online content moderation*, in *Computer Law & Security Review*, 2020, vol. 36, § 4). La proposta, teoricamente interessante, concretamente contrasta però in modo frontale con il diritto di difesa, costituzionalmente tutelato (art. 24 Cost.), che non può essere inibito, e presuppone un radicalmente diverso modello di business per le piattaforme: fa pensare ai <modelli di organizzazione dell'ente>, di cui all'art. 6 d. lgs. 231/2001. Solo che ciò comporterebbe la necessità di vagliare non solo la procedura di trattamento della contestazione, ma anche l'algoritmo che governa il newsfeed (che infatti deve essere trasparente, secondo Hartmann I.A.: p. 9). Si fa notare da più parti che la moderazione avviene sempre in prima battuta tramite segnalazioni (*flagging*) degli utenti: i quali dunque "*are integral to the flagging system, making them "uncompensated digital labourers" who are unaware of the services they deliver to the platform along with access to their valuable personal data*" (MacKenzie F. Common, *Fear the Reaper: how content moderation rules are enforced on social media*, in *International Review of Law, Computers & Technology*, 2020, 34:2, p. 128 (che scrive di *crowd-sourced enforcement*; Morozov, ivi cit., scrive di *crowd-sourced censorship*). Non mancano abusi pure nelle attività di *flagging* (Kaye D., *The global struggle to govern the internet*, cit., 62-63).

rivals' emergent services and products to avoid any contraction of their market share. They also routinely rely on intellectual property law (such as patent and trade secrets laws), worker contracts (such as nondisclosure and noncompete agreements), and a wide assortment of other legal tools to preserve control over their internal decisionmaking processes. And, besides all of this, they also appeal to the variety of governments and jurisdictions around the world where their users reside, including authoritarian regimes with no compunction about imposing restrictions on political speech>>[358]. La content moderation dunque è un processo non statico, ma frutto di una negoziazione continua tra una pluralità di attori: policy teams, moderatori assoldati, user communities, governi, inserzionisti, mass media, civil society groups e esperti accademici. In pratica, è guidata da almeno "*four sets of influences—corporate philosophy, regulatory compliance [a precetti mandatory o anche solo informal], profit maximization, and public outcry—each of which affects what is possible, permissible, and visible on online platforms*"[359].

Tuttavia la situazione non sembra allo stato evitabile, dato che, da un lato, le comunicazioni avvengono in misura preponderante tramite essi e, dall'altro, i provider sono nella miglior posizione tecnico-economica per prevenire o limitare i danni: per cui è ovvio che saranno i medesimi a procedere in prima battuta al bilanciamento predetto[360]. Attribuir loro il dovere di intervento, dopo ponderazione degli opposti interessi nel singolo caso, appare allo stato giustificato o almeno non

[358] Sylvain O., *Recovering tech's umanity* in *Columbia law review*, 2019, vol. 119/7, pp. 264/5, ove recensione critica di Wu T., *Will Artificial Intelligence Eat the Law? The Rise of Hybrid Social-Ordering Systems, Columbia Law Review*, 2019, vol. 119/7, perché, troppo incentrato sul problema dell'interazione uomo-algoritmo nella presa di decisioni sociali significative, dimentica l'imponente sforzo di attività prettamente umane che pur esistono nelle Big Tech, anche allo scopo di sfruttare la loro posizione di intermediari tra utenti e advertisers (p. 266 e in generale parte III e IV).

[359] così Sander B., *Freedom of Expression in the Age of Online Platforms*, cit., p. 498 ss.. Il *public outcry* va fatto rientrare nella profit maximization, in quanto l'impresa lo conteggierà nella misura i ncui inciderà sui profitti.

[360] Tra i molti v. Suzor N.P., *Lawless. The secret rules that govern our digital lives*, cit., p. 7.

evitabile[361]. Del resto la situazione non è nuova: non tanto diversa, infatti, sotto questo profilo (anche se assai più ridotta in termini quantitativi ed invece più estesa in termini di controllo dei contenuti[362]), era la situazione degli editori circa i contributi informativi ospitati. A meno di optare per soluzioni pubblico-dirigistiche (di natura vagamente espropriativa) delle relative attività di impresa, che dovrebbero però essere attentamente vagliate.

20. Inevitabilità del ruolo decisorio (e quindi censorio) su diritti soggettivi. Applicabilità dei diritti fondamentali anche verso enti privati come le piattaforme

In sintesi, allora nessuna stranezza se anche l'intermediario sia chiamato a fare valutazioni simili a quelle che le cit. sentenze demandano al giudice o all'editore. Come detto, la differenza rispetto all'editore è che il dovere (e/o onere) in tale senso sorge in capo al provider solo dopo che abbia "effettiva conoscenza" dei fatti: in pratica, dopo che sia stato avvisato dal titolare del diritto leso (anche se la notizia che fa scattare l'obbligo di rimozione/disabilitazione può arrivargli da qualunque fonte, direi). Il ruolo censorio delle grandi piattaforme (social network, soprattutto, ma pure motori di ricerca, mutatis mutandis)[363] nel

[361] Rileva questa posizione di bilanciamento pure Petruso, R., *La responsabilità degli intermediari della rete telematica*, cit., 241 ss, per cui l'avversione del provider al rischio tendenzialmente lo indurrà ad accogliere la domanda di rimozione (ivi, p. 247). Questo però avviene perchè egli vede il rischio solo da parte del titolare, che si allega leso, e non da parte dell'upoloader: bisogna allora chiedersi quali siano le ragioni di ciò e la risposta è articolata (a prima vista: maggior forza economica e organizzativa dei titolari delle privative itnellettuali, solitamente nella parte degli istanti, rispetto a privati o artisti sconosciuti; giurisprudeznza ancorata a schemi tradizionali; scelta normativa di safe harbour solo per la rimozione ma non per l'opposto caso e assenza di sanzioni per l'illegittima istanza di rimozione/disabilitazione; etc.). Venendo meno tali ragioni, cambiebbero pure gli incentivi per i provider a decidere nel senso anzidetto.

[362] A questa osservazione si potrebbe opporre che la situazione in fondo non è molto dissimile tra editore e piattaforma hosting provider: è questa infatti, in base agli algoritmi governanti il newsfeed, che alla fine decide cosa ciascuno può vedere dei post altrui. Tuttavia ciò potrebbe valere solo fino ad un certo punto: ad es. si potrebbe ipotizzare di ingannare l'algoritmo con opportuni post apparentemente bizzarri. Ciò nonostante i contenuti resterebbero determinati solo dallo strumento tecnologico creato dalla piattaforma.

[363] V. il ranking dei principali social, con i tassi di diffusione, in statista.com e in https://makeawebsitehub.com/social-media-sites/. Gli studiosi di marketing fanno notare in proposito la differenza tra Europa e Stati Uniti, da una parte, e

pubblico dibattito di idee, oggetto dei primi studi, è fonte di preoccupazione[364] e dovrà essere ridimensionato oppure controllato, già giudizialmente prima che legislativamente: ad es. riconoscendole come luogo aperto al pubblico, in cui non si può impedire la libertà di riunione digitale o di parola, oppure come mass media la cui disciplina obbliga il gestore alla tutela del pluralismo[365], aggiornando la questione dell'applicabilità ai

Russia, Cina e Giappone, dall'altra (Kotler Ph-Hollensen S,-Prensik M.O., *Social media marketing. Marketer nella rivoluzione digitale*, Hoepli, 2019 (orig.: 2019), 48 (nel secondo gruppo inseriscono pure la Germania con Xing, social professionale simile a Linkedin). Anche il market place (di Amazon) funziona in modo del tutto analogo ai motori di ricerca: di fronte ad una domanda, offre in risposta una serie di proposte commerciali, che necessariamente sono mostrate in elenco, il cui ordine è essenziale per la visibilità.

[364] "*Super-intermediaries: A road block for free information*" titola il § III.C del suo saggio Criscione H., *Forgetting the Right to be Forgotten: The Everlasting Negative Implications of a Right to be Dereferenced on Global Freedom in the Wake of Google v. CNIL*, 32 Pace Int'l L. Rev. 315 (2020), 348 ss (l'a. è poi molto critico verso la UE per le sue pretese di applicazione extraterritoriale della propria disciplina di data protection, al punto di scrivere di *data imperialism*: p. 351 ss).

[365] Queste le due ricostruzioni più plausibili per M. Monti, *Privatizzazione della censura e Internet platforms: la libertà d'espressione e i nuovi censori dell'agorà digitale*, in *Riv. it. inform. e dir.*, 2019/1, 35 ss, 44. Potrebbe anche alternativamente ipotizzarsi la parificazione dello spazio digitale al luogo fisico e dunque la presenza sulla piattaforma al diritto di riunione ex art. 17 Cost. in luogo pubblico o –meglio- privato aperto al pubblico oppure al mero assembramento (cenni sulla legislazione inerente il luogo privato aperto al pubblico nel t.u.p.s. in Barbieri G.T., Art. 17, in Bifulco-Celotto-Olivetti (a cura di), *Commentario alla Costituzione*, Utet, I, 2006, 382 ss, sub § 2.8; per l'a., poi, il diritto di assembramento rientra in quello di riunione, § 2.10), come la dottrina ha già sottolineato (così, circa i social network, Allegri M.R., *Ubi social, ibi ius*, cit., 44 ss; l'a. ammette pure la qualifica di formazione sociale ex art. 2 Cost., p. 29 s. nonché in certi casi –*social network communities*- di associazioni ex art. 18 Cost., p. 37 ss). L'art. 21 c.1 Cost. (come l'art. 15 c. 1 Cost) non limita l'esercizio del diritto di parola ad ambienti pubblici in senso stretto, per cui mi pare senz'altro applicabile anche ad ambienti privati (conf. Pace A., in Pace A.-Manetti M., *Art. 21 La libertà di manifestazione del proprio pensiero*, in Branca (a cura di), *Commentario della Costituzione*, Zanichelli-Il Foro italiano, 1978, pp.37/38, testo e nota 2, secondo cui si tratta di tesi pacifica in dottrina; Mostacci E., *Critica della ragione algoritmica: internet, partecipazione politica e diritti fondamentali*, costituzionalismo.it, 2019/2, 80-82,) quanto meno quando –regole di ingresso o meno- acquisiscono nei fatti importanza fondamentale (in positivo e in negativo, cioè quanto ad opportunità e a rischi) per la vita delle persone, tenuto conto che non si vedono motivo per escludere le disposizioni costituzionali dall'intepretazione evolutiva (Repetto G., *Premesse ad uno studio sull'interpretazione evolutivatra costituzione e convenzione europeadei diritti dell'uomo*, in Cassetti L. (a cura di) *Principi e garanzie sotto la lente dei giudici di Strasburgo*, Jovene, 2012, 21 ss, §§ 2-3, letto in academia.edu): e ciò sia come

diritto di esprimersi che di informazione attiva e passiva (l'uno e gli altri da equipararsi: M. Orofino, *Art. 21 Cost.: le ragioni per un inervento di manutenzione ordinaria*, medialaws.eu, 2019/2, 23.07.2019, 84-85), dovendosi tutelare anche chi desidera ricevere –per scelta intellettuale o per dovere profesionale- informazioni dei più vari orientamenti (si v. la sintesi sull'estensione dello *State action doctrine* alle internet platforms nel diritto Usa in M. Monti, *Privatizzazione della censura*, § 3.1; la freedom of expression pone le questione centrali nel diritto costituzionale oggi secondo J.M. Balkin, *Free Speech in the Algorithmic Society*, cit., 1158). I c.d. *social* sono infatti ambienti sì privati ma che spingono potentemente per tale apertura nella misura massima possibile (ad es. <<*Il ruolo di Facebook Ireland in relazione alla condivisione di dati tra utenti e app di terzi attraverso il "Facebook Login" è in ultima analisi quello di un intermediario online, che facilita le scelte di condivisione dei dati liberamente effettuate dagli utenti, coerentemente con la loro libertà di manifestazione del pensiero e con l'interesse pubblico di favorire la libera circolazione dei dati (…) Facebook è un social network la cui missione è " dare alle persone il potere di costruire una comunità e di avvicinare il mondo". E' carattere intrinseco di un social network - è nella sua natura - che gli utenti si registrino allo scopo di reperire e condividere informazioni con i loro amici e familiari esistenti e con i loro futuri contatti"*>>: cosi nella sintesi della difesa di Facebook riportata nell'ordinanza–ingiunzione 14.06.2019 del Garante Privacy nei confronti di Facebook Ireland Ltd e Facebook Italy s.r.l., pp. 4-5: ma non c'è bisogno di dare evidenza di ciò, costituendo fatto notorio, probabilmente pure ex art. 115 c.2 cpc), irrilevante essendo che lo facciano per motivi di lucro. L'invocabilità dei diritti inviolabili nelle formazioni sociali è del resto esplicita nell'art. 2 Cost., su cui v.: Pizzorusso A., *Art. 1-4*, in Pizzorusso ed altri, *Art. 1-10 Delle persone fisiche*, in *Comm. cod. civ. Scialoia Branca* a cura di Balgano, Zanichelli- Il foro, 1988, 210-215; Rossi E., sub art. 2, in *Comment. alla Cost.* dir. da Bifulco-Celotto-Olivetti, Utet, 2006, 1, sub § 2.2.2-2.2.3, 52-54, che eccettua dal diritto di free speech le organizzazioni di tendenza; Basile M., *Le persone giuridiche*, t. I, in Tratt.dir. priv. a cura di Iudica-Zatti, Giuffrè, 2020, 3 ed., 381, per cui la giustizia interna non è esclusiva in caso di lesione di diritti inviolabili; Barbera A., *Art. 2*, in Aa.Vv., *Principi fondamentali. Art. 1-12*, in *Comm. della Cost*. a cura di Branca, Zanichelli-Il foro it., 1975, 107 e 113-116 (ammettendo però distinzioni e in particolare eccettuando i moderni *Principi* (sic!), la cui "immunità" sarebbe "ormai un dato della <costituzione materiale>>, p. 115). Del resto i partiti c.d. digitali (Movimento 5 Stelle da noi e Podemos in Spagna, oltre che i c.d. Partiti Pirata), per l'organizzazione, centrata essenzialmente su piattaforma digitale, ricorderebbero da vicino le Big Tech (Gerbaudo P., *I partiti digitali*, cit., passim, spt. cap. 3, p. 89 ss e p. 231 ss: il giudizio è però questionabile, ricorrendo si la fame di dati, ma mancandone il tratto principale, costituito dallo scambio *servizi internet contro cessione del diritto sui propri dati*). Opta per la tutela basata sui limiti costituzionali alla libertà d'impresa ex art. 41 Cost., più favorevole di quella basata sui diritti inviolabili nelle formazioni sociali ex art. 2 Cost., Cuniberti M., *Potere e libertà in rete*, Riv. dir. media, medialaws.eu, § 3: per l'a., il secondo approccio trascura il differente ruolo degli intermediari rispetto a quello degli utenti e vela la centralità del loro soverchiante potere economico (resta però il problema dell'applicabilità anche immediata dell'art. 41 c.2 Cost. oppure solo intermediata da legge). L'estensione della *state action doctrine* alle piattaforme è ora sostanzialmente affermata dalla Corte Suprema in *Packingham v. North Carolina*, No. 15–1194. Argued February 27, 2017—Decided June 19, 2017

(come riferisce l'ottimo lavoro di Klonick K., *The New Governors: The People, Rules, and Processes Governing Online Speech, Harvard Law Review*, vol. 131, Aprile 2018, n.6, 1610-1611), e spt. l'opinione dei giudici Kennedy e Alito. Con la conseguenza che l'account Tweet –anzi lo spazio di replica ad ogni singolo tweet- del Presidente Trump- costituisce *public forum* e la disabilitazione di un cittadino all'accesso di tale spazio viola la freedom of speech che deve esservi permessa: così *Knight First Amendment Inst. at Columbia Univ. v. Trump*, No. 18-1691-cv, United States Court of Appeals for the Second Circuit, Decided Jul 9, 2019 (ne riferisce Nunziato Dawn C., *From Town Square to Twittersphere: The Public Forum Doctrine Goes Digital*, 25 *Boston University-Journal of Science & Technology Law* (2019), Forthcoming, letto in ssrn.com, 68-69; esame della public forum doctrine alle pp. 22 segg., pur se la sentenza è stata impugnata dalla Casa Bianca come riferisce un post 20.20.2020 dello stesso *Knight First Amendment Instititute*); però il Presidente ha dato esecuzione incompleta, sbloccando solo alcuni account, per cui il Knight Institute ha riproposto l'azione il 31.07.2020, caso 1:20-cv-05958, come da comunicazione in pari data, ove anche il testo del nuovo *complaint*; di altri due casi con esito l'uno analogo e l'altro opposto –pagina Fb della contea di Loudoun in Virginia e rispettivamente account Twitter del governatore del Kentucky- rifersce Reade N., *Is there a right to tweet at your President?, Fordham law review*, marzo 2020, vol. 88/4, 1473 ss, 1490-1496 (l'a. è contrario alla qualifica dei social come *public forum*, stante la loro natura di impresa editoriale, pp. 1501-1504: il che è discutibile, se si paragona il titolo giuridico che li lega agli utenti-uploaders rispetto a quello che lega editore e suoi dipendenti/collaboratori e comunque dovrebbe seguirne –da noi- la gravosa c.d. responsabilità editoriale civile e penale); la giurisprudenza statunitense fa passi indietro con Corte Suprema USA, Manhattan Community Access Corp. Et al. V. Halleck et al., No. 17–1702, 7 giugno 2019, annotata criticamente da D. Zecca, *I canali a pubblico accesso non sono un public forum: i perché di un'occasione persa*, 22.01.2020, in medialaws.eu: in una lite sull'esclusione di due newyorkesi dalla fruizione dei canali TV via cavo ad accesso pubblico, disposta dalla società privata affidataria del sercizio, la Corte ha rigettato l'istanza di accesso dei primi, ancorandosi al dato formalistico dell'affidamento della gestione ad un soggetto non pubblico ma privato: non valorizzando il fatto che la scelta di creare canali ad accesso pubblico era imposta dalla legge e che il privato era intervenuto per una scelta discrezionale della città di New York, la quale gli aveva imposto diverse limitazioni (v. sub II.C). In tale modo si condiziona il diritto di accesso ad un canale pubblico alla scelta della P.A. sul se procedere con affidamento all'esterno oppure in house! (si v. anche sub II.B sul fatto che un privato, che organizza un qualche forum speech, per questo solo non diventa *state actor*) (decisione a stretta maggioranza: 5-4). Altro passo indiertro in una sentenza della California Trial Court in *Johson v. Twitter*, 6 giugno 2018, allorchè la Corte ha rigettato l'impugnazione della chiusura di un account (per frasi aggressive e minacciose) disattendendo l'argoimento della *state action* e della paragonabilità ad un noto caso del 1979 di raccolta firme in uno shopping mall (*Robins v. Pruneyard Shoping Center*): solo che lo fa con motivazione scarna (forse assente) e cioè semplicemente opponendo che non si trattava della stessa situazione, dato che il tweet era "threatening and harassing", per cui Twitter bene ha fatto a rimuoverlo, esercitando –in sostanza- il suo diritto di parola (coperto dal Primo Emendamento) e di impresa editoriale, anche a tutela dei suoi utenti. Ulteiore passo indietro con US Court of Appeals for the ninth circuit, 26.02.2020, *Prager University c. Google-Youtube*, secondo cui seccamente <<*despite YouTube's*

ubiquity and its role as a public-facing platform, it remains a private forum, not a public forum subject to judicial scrutiny under the First Amendment… That YouTube is ubiquitous does not alter our public function analysis>> (p. 5 e 11), per cui va rigettato il *First Amendment claim*, poiché Youtube, ente privato, non è qualificabile come entità governativa né *public forum* né *company town* (rif. a *Marsh v. Alabama*, 326 U.S. 501, 505–09 (1946)) né svolge una funzione pubblica (ivi, p. 10 nota 3, cit. di altre sentenze recenti conformi). Estende ai social media la tutela del pluralismo, affermata da due sentenze della Corte Suprema per la radio (Red Lion Broadcasting Co v. FCC del 1969 e FCC v. Pacifica Foundation del 1978), ricorrendo la stessa ratio, Suozzo C.J., *Red Lion Broadcasting Co. V. FCC and the Rise of Speech-Enhancing Regulations of Social Media Platforms*, 4 *Georgetown Law Technology Review* (2019) 215 ss, spt. sub III, 225 ss. Negli USA, se non si può azionare la *state Action doctrine* federale contro la piattaforma, in quanto soggetto totalmente privato, come molti affermano, si può però invocare l'analoga –ma spesso più favorevole- regola presente nelle Costituzioni dei singoli Stati (O'Kelley E., *State Constitutions as a Check on the New Governors: Using State Free Speech Clauses to Protect Social Media Users from Arbitrary Political Censorship by Social Media Platforms*, in *Emory Law Journal*, 2019, vol. 69/1, 111 ss.; per l'a. le piattaforme non possono invocare lo scudo del § 230 Decency Act per la rimozione di post politici, in quanto non rientranti nella fattispecie di cui al punto c.2.A del § 230: pp 158-160): ipotesi però da noi non percorribile. In breve, non dovrebbe esserci dubbio che la tutela dei diritti fondamentali operi immediatamente (unmittelbare/direkte Drittwirkung) non solo verso il potere statale ma anche verso i poteri privati, dato che le c.d. Big Tech aspirano ad allargare sempre più il loro ruolo di governo, sostituendo *the logic of territorial sovereignty with functional sovereignty. In functional arenas from room-letting to transportation to commerce, persons will be increasingly subject to corporate, rather than democratic, control* (F. Pasquale, *From Territorial to Functional Sovereignty: The Case of Amazon*, 06.12.2017, Law and Political Economy blog). In pratica, un diritto non solo al *delisting*, come fatto in Google Spain (così riconoscendo efficacia orizzontale ai diritti fondmentali: M. Bassini, *Fundametnal rights and private enofrcement in the digital age*, in *European law journal*, 2019, 195), ma anche –all'opposto- ad una reindicizzazione di visibilità pari a quella anteriore o ad una nuova messa on line del post. Per non dire che le clausole di riserva della piattaforma del diritto di oscurare (in tutto in parte) sarà probabilmente nulla o male invocata: v. l'affermazione in tal senso di Trib. Roma ord. 12.12.2019, RG 59264/2019, CasaPound c. Facebook, cit., p. 4. Il problema, come detto, è però quello dell'abissale disparità di forza contrattuale, ragion per cui serve un'azione statale meglio di più Stati, dato che uno da solo potrebbe non avere forza necessaria (così pure Cassese S., *Il buongoverno. L'età dei doveri*. Mondadori, 2020, 62), anche per gli inevitabili tentativi di regulatory capture praticati (Petrillo P.L, *Teorie e tecniche del lobbying*, Mulino, 2019, 288 ss, pur favorevole in generale all'attività di lobbying correttamente intesa, legittima ed anzi indice di democraticità del sistema: p.11; R. Foroohar, *Release Big Tech's grip on power. Silicon Valley is defending a business model that looks a lot like rent-seeking*, Financial Times, www.ft.com, 18.06.2017, <<*But our biggest technology conundrum — what to do about the fact that Silicon Valley holds too much economic and political power — isn't on the agenda. No wonder. Over the past few years, Big Tech has quietly become the dominant political lobbying power in Washington, spending huge amounts of cash and exerting serious soft power in an effort to avoid regulatory*

disruption of its business model, which is now the most profitable one in the private sector>>); azione statale magari antitrust (nel cui campo rientra l'informazione economica –non quella socio-politica-: Day G. *Monopolizing free speech*, in *Fordham law review*, marzo 2020, vol. 88/4, 1315 ss, spt. 1336 ss e la parte IV.A a 1345 ss) ma probabilmente insufficiente e dunque da accoppiare a regolamentazione, come osserva A. Perrucci, *Dai Big Data all'ecosistema digitale. Dinamiche tecnologiche e di mercato e ruolo delle politiche pubbliche*, Anal. giuridica Econ., 2019, 1, 82, sulla base del *Competition Policy for the digital era. Final report*, by J. Crémer- Y.A. de Montjoye-H. Schweitzer, Commissione Europoea, 2019 (ad es. § 3.5 e § 7 Conclusioni; v. anche l'interessante passo sui poteri regolatori delle piattaforme al § 4.III Platforms as regulators (competition on the platform), il qiale cautamente osserva <<*La possibilità che – pure in mercati concorrenziali – possano determinarsi restrizioni o limitazioni al pluralismo dell'informazione, già riconosciuta dal Legislatore, diviene più probabile con l'evoluzione digitale dei mercati dell'audiovisivo*>> (propone la forzata dispersione dell'azionariato o covnresione a modelli non profit del tipo public utilities, K. Basu, *How to tame Big Tech*, project-syndicate.org, 31.10.2019 (questo va osservato circa la pur astrattamente condivisibile affermazione di Libertini, *Sulla nozione di libertà economica*, Contr. impr., 2019, 4, 1285, per cui -contro i rischi di riduzione democratica prodotti dalla concentrazione di poteri economci- è opportuina la presenza di poteri pubblici forti e da essi indipedenti, per proteggere, secondo la teria ordoliberale, l'efficienza dei mercati anziché le imprese esistenti in quanto tali: spesso il singolo Stato faticherà a fronteggiare i giganti del web); un esame comparato delle possibilità di intervento in Rochefort A., *Regulating Social Media Platforms: A Comparative Policy Analysis*, Communication Law and Policy, 2020, 25:2, 225-260 (che sarebbero: *industry self-regulation*, *limited government regulation*, *comprehensive government regulation* e cioè come *Public Utility*, *break up major platforms* e GDPR: v. sintesi in tabella 2, p. 238/9); sulle difficoltà delle Autorità Regolatorie statali a trattare i problemi posti dalle grandi piattaforme v. Cohen J.E., *Law for the platform economy*, cit., sub III.B., 184 ss. O quanto meno –per il limitato obiettivo della riservatezza oggetto di atto dispositivo- servono adeguate azioni private collettive o ammnistrative dei Garanti privacy (si v. da ultimo quella promossa dal Consumer Watchdog australiano contro Google per la tracciatura dei dati di geolocalizzazione: J. Smyth, *Australia sues Google over consumer location privacy*, *Financial Times*, *www.ft.com*, 29.10.2019). La creazione da parte di Facebook di un Oversight Board indipendente (F.O.B.; sul processo creativo v. in dettaglio Klonick K., *The Facebook Oversight Board*, cit., parte II, 2448 ss.) con funzioni censorie in seconda istanza, da un lato costituisce riconoscimento del ruolo paracostituzionale della piattaforma (lo stesso Zuckerberg si espresso intale senso paragonando il suo F.O.B. alla Supreme Court -anche se poi ha cessato tale paragone: così si legge in E. Douek, *Facebook's "Oversight Board:" Move Fast With Stable Infrastructure And Humility*, North Carolina Journal Of Law & Technology, vol. 21, Issue 1, Oct. 2019, 17 e 29; reputano vigorosamente le Big Tech dei *quasi-governmental actors* Kim N. S.-Telman D.A. J., *Internet Giants as Quasi-Governmental Actors*, cit, parte II, 744 segg., rilevando che cumulano i poteri del soggetto pubblico con l'irresponsabilità e opacità del privato, e li reputa *transnational sovereigns* Cohen J.E., *Law for the platform economy*, cit. in questa nota, 199 ss), ma dall'altro parrebbe un'operazione di facciata o meglio un passo il più modesto possibile per rallentare l'avanzata di opinioni critiche, che possono portare a limitazioni legislative, o per

distrarre da temi più spinosi come l'ammissibilità della gestione algoritmica o –soprattutto- direi- del microtargeting (Klonick K., *The Facebook Oversight Board*, cit., 2426/7 e 2488). Un organo seriamente indipendente ad es. avrebbe dovuto prevedere la nomina (di almeno una buona minoranza) dei suoi componenti da parte di enti esterni difficlmente catturabili come ad es. qualche Watchdog statale o del Garante europeo della protezione dei dati, dato il ruolo guida in materia esercitato dalla UE (opinione diffusa: Pernot-Leplay E., *EU Influence on Data Privacy Laws: Is the US Approach Converging with the EU Model?*, in *Colorado technology law journal*, vol. 18/1, 2020, sub I.A, p. 27 ss; Schartz P.M., *Global Data Privacy: The EU Way*, *N.Y. Univ.Law review*, 94/3, Oct. 2019, 771 ss, passim, spt. cap. I; Klonick K., *The Facebook Oversight Board*, cit., 2490 lamenta l'assenza di ogni *voice* in capo agli utenti). Soprattutto però avrebbe dovuto dare poteri ad un Board indipendente non solo su qualche reclamo ma anche sul cuore del business e cioè degli algoritmi che determinano i newsfeed e il microtargeting pubblicitario: che invece restano segretissimi, per cui all'azienda sarà facile aggirare le decisioni eventualmente non gradite del Board: simile riflessione leggo nell'interessante lavoro di E. Douek, *Facebook's "Oversight Board*, cit., p. 43 e 47 segg. (anche se enumera dei vantaggi a 58 segg.; v. poi qui da un lato le quattro ragioni di convienenza per cui FB ha deciso di creare la struttura F.O.B., sub II.B, 16 segg., e sub IV p.46, e dall'altro l'esame dei seguenti profili del F.O.B.: membership, power of reviews, subject-matrer jurisdiction, degree of algorithmic transparency) (v. ora post 28.01.2020 del manager di FB Brent Harris; altre perplessità sul F.O.B. in article19.org). Perplessità sul F.O.B. in: - Pollicino O., *L' "autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, www.federalismi.it, n. 19/2019 del 16.10.2019, 10-11; - Douek E., *What Kind of Oversight Board Have You Given Us?*, Univ. of Chicago law review online, 11.05.2020; - nel Rapporto Kaye *Research Report by the Mandate of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* per l'ONU, luglio 2020, sub B Preliminary Analisis, § 35 ss., oltre che Facebook ha creato un sito apposito: (https://www.oversightboard.com. Una panoramica sull'autoregolamentazione dei principali social su temi politici in Bonini P., *Social Network. Una prima ricognizione delle regole sui contenuti politici* in *Federalismi*, 2020/11, 24.04.2020, in federalismi.it., concludendo per la necessità di regolamentazione specifica (§ 4, p. 280 ss). Il sistema di filtraggio automatico e manuale è accuratamente esaminato da K. Klonick, *The New Governors*, cit., 1630 ss e spt. 1635 ss. e da MacKenzie F. Common, *Fear the Reaper*, cit., che giudica il lavoro di Klonick troppo ottimistico sulla qualità della content-moderation svolta dalle piattaforme (p. 129 e 137/8, §2 e § 3 sui bias cognitivi inevitabili). Klonick si chiede perché le piattaforme, pur potendo fruire di un ampio safe harbour quale quello del § 230 del *Communications Decency Act* del 1996 – title 47 U.S. Code, impegnino molte energie per migliorare di continuo il funzionamento del sistema di moderazione dei contenuti (p. 1617 ss): e la risposta –non difficile- consiste soprattutto nell'evitare il rischio di una regolamentazione statale imperativa (Frosio G.-Husovec M., *Accountability and Responsibility of Online Intermediaries*, 2019, 14, in Frosio G. (ed.), *The Oxford Handbook of Online Intermediary Liability*, Oxford University Press, 2020, Forthcoming, legibile in ssrn.com) e/o in motivi economico-reputazionali (K. Klonick in *The New Governors*, cit., p. 1627 e in *The Facebook Oversight Board*, cit., 2426/7; conf.. Citron Keats D.-Norton H., *Intermediaries and Hate Speech: Fostering*

Digital Citizenship for Our Information Age, *Boston University Law Review*, Vol. 91, 2011, p. 1453 ss.; Holliday E.M., *Missing Links: The First Amendment's Place in an Everchanging web*, in *Pittsburg Journal of Technology Law & Policy*, XIX, 2018-2019, 61) per mantener o incrementare la *Community* (J.M. Balkin, *Free Speech in the Algorithmic Society*, cit., passim, ad es. 1162, 1181, 1183, 1195), soprattutto per il rischio di minor vendibilità degli spazi pubblicitari immancabilmente e necessariamente connessi ad ogni servizio da esse fornito in via apparentemente gratuita (ad es. G. De Gregorio, *Democratising online content moderation*, cit., 2). In modo singolarmente analogo allo *Statement on the Purpose of a Corporation* dei CEOs delle più grandi corporation appartenenti alla Business Roundtable, 19.08/06.09-2019, rilasciata verosimilmente per cercare di prevenire il diffondersi di reazioni contro le diffuse malefatte (v. J.E. Stiglitz, *Is Stakeholder Capitalism Really Back?*, 27.08.2019, project-syndicate.org e M.Roe, *Why America's CEOs Are Talking About Stakeholder Capitalism*, 04.11.2019, project-syndicate.org). Anche per tale scopo, però (oltre che per creare quanti più spazi pubblicitari: v. sopra), servono quanti più dati possibile, dato che <<*the system needs to be trained. The more data that is fed into it — whether images of terrorist insignia or harmful keywords — the more the machine learning technology learns and improves. Without enough training data, the system does not know what to look for*>> (H.Murphy-M. Murgia, *Can Facebook really rely on artificial intelligence to spot abuse?*, 08.11.2019, *Financial Times*, www.ft.com): I due cit. obiettivi (va menzionato pure il c.d. filtraggio collaborativo in piattaforme come Netflix, Spotifym Yoyutube: la rilevazione delle preferenze, date con le playlist anche da utenti free, permette di affinare l'algoritmo per gli utenti premium: spiegazione in A. Vespignani con R. Rijtano, *L'algoritmo e l'oracolo*, cit., 81-2; pure se la review degli utenti serve a Facebook anche a superare la notevole difficoltà degli algoritmi nell'individuare le sfumature linguistche necessarie per accertare molestie e hate speech: Kadri T.E.-Klonick K., *Facebook v. Sullivan*, cit., 59), strumentali a quello ulteriore e finale, che è unico (profitto, se possibile durevole) richiedono la medesima vorace accumulazione di dati, alla luce del ruolo giocato dal c.d. effetto di rete (su cui v. AGCM-AGCOM-Garante Privacy, *Indagine conoscitiva sui* Big Data, cit., p. 93, § 5.3.5). Per cercare di risolvere i gravi problemi (cinque ne elencano: Sabeel Rahman K.-Teachout Z., cit. subito dopo, p. 12) generati dall'inedito abbinamento in capo alle piattaforme (Google e Facebook, soprattutto) del potere di tracciare i singoli in modo precisissimo e di governare a proprio profitto il flusso informativo per larga parte della popolazione mondiale, alcuni studiosi hanno proposto di introdurre il divieto di pubblicità personalizzata (microtargeting), suggerendo allora che il sostegno finanziario (son pur sempre imprese private!) tornasse ad essere …. il pagamento di un corrispettivo: Sabeel Rahman K.-Teachout Z., *From Private Bads to Public Goods: Adapting Public Utility Regulation for Informational Infrastructure. Dismantling surveillance-based business models, 04.02.2020, Knight First Amendment Institute.Columbia University* (spt. 16-18; il paper contiene un breve ma chiaro sunto della questione) (idea non peregrina, pare, dato che il capo economista di Google, Hal Varian, prevede che alla fine andrà proprio così, come riferisce Srnick N., *Capitalismo digitale*, cit., p. 105). L'idea del pagamento troverebbe resistenze tra gli utenti, se è vero che, secondo sondaggio USA, sono disposti a pagare non oltre $ 1 di mediana e $ 7,38 di valore medio al mese per fruire di Facebook, c.d. *willingness to pay*, anche se il prezzo sale di molto, secondo l'effetto dotazione studiato dall'economica comportamentale, nell'opposta situazione del prezzo cui sarebbero disposti a rinunciarvi, c.d.

mezzi di informazione privati del dovere di garantire il c.d. pluralismo interno[366]. La mancanza di alternative significative ai social media (o al motore di ricerca, mutatis mutandis), produce alcune conseguenze di rilievo, tra cui ad es.: i) legittima interventi governativi, senza rischio di censure per violazione del Primo Emendamento (basate sulle policies potenzialmente discriminatorie –per alcuni- delle piattaforme)[367]; ii) soprattutto, comporta che la libertà di espressione c'è solamente finche essi la tollerano. L'ordinamento dovrebbe fare un'eccezione alla *state action doctrine* o meglio estenderla, quando il potere privato diventa così grande da minacciare la libertà allo stesso modo in cui può farlo uno Stato[368] (anche per la sua tutt'altro che nitida costruzione[369]): conclusione ineccepibile, se si pensa che

willingness to accept (così l'interessante Sunstein C., *Valuing Facebook*, in *Behavioural Public Policy*, 2019, 1-12, passim). La profilazione dà luogo ad un marketing predittivo, per cui ad es. si parla di *anticipatory selling* (proposte di prodotti che il cliente nemmeno conosceva: ma questo in fondo non è così nuovo …) e soprattutto di *anticipatory shipping* (stoccaggio anticipato in magazzini collocati nei luoghi più idonei in base alle preferenze rilevate dalla geolocalizzazione): così apprendo da Talia D., *La società calcolabile e i big data*, cit., 25 (il quale a p. 22 ricorda che, secondo lo storico Eric Hobsbawm, il plusvalore del nuovo millennio non è più generato dagli operai ma dai consumatori digitali: i quali pagano col loro tempo e con la loro attività di utenti e di contributori marginali dei contenuti il costo della realizzazione dei servizi fruiti, generando profitto per i nuovi padroni del vapore digitale).

[366] Cuniberti M. in Vigevani G.E. ed altri, *Diritto dell'informazione e dei media*, Giappichelli, 2019, 249; Zaccaria R.-Valastro A.-Albanesi E., *Diritto dell'informazione e della comunicazione*, Cedam, 2016, 9 ed., p. 51-53.

[367] E' il problema discusso da Telegen M., *You Can't Say That!: Public Forum Doctrine and Viewpoint Discrimination in the Social Media Era*, *University of Michigan Journal of law reform*, vol. 52/1, 2018, 234 ss: il divieto di hate speech, previsto da tutte le policies, costituirebbe discriminazione di punti di vista/viewpoint discrmination (Corte Suprema *Matal v. Tam*, 137 S. Ct. 1744, 1763 del 2017): la quale andrà attribuita pure al governo, se sceglie di usare le piattaforme. La tesi non persuade: da un lato, l'uso della piattaforma più usata al mondo non pare di fatto rinunciabile per sentire punti vista dei cittadini e, dall'altro, il diritto di free speech va conciliato con altri diritti (almeno da noi probabilmente prevalenti, ma credo ormai almeno equipotenti pure negli USA), che l'hate speech lederebbe. L'a. elabora una proposta conciliativa non troppo lontana da quanto qui osservato (Telegen M., op. cit., parte III, 254 ss.): va ammesso ciò che rientra nel *normal usage* della piataforma, tale essendo quello non probito [da altra disposizione] (p. 262/3).

[368] Così l'interessante saggio di Domer P., *De Facto State: Social Media Networks and the First Amendment*, cit., 919 e 923.

[369] Sumrall A.C., *Epiphenomenal or Constructive?: The State Action Doctrine(s) and the Discursive Properties of Institutions*, Texas law review, vol.

le piattaforme <<*are becoming global arbiters of free speech*>>[370] e che il divario, tra chi controlla le tecnologie e chi non vi ha accesso, diventerà incolmabile[371]. Ovvero, gli interpreti dovrebbero interpretare evolutivamente il concetto, dato che l'assimilazione delle dominant platforms agli Stati nei loro requisiti costitutivi tradizionali, ha guadagnato crescenti consensi[372], tenuto conto che condizionano significativamente e unilateralmente la vita delle persone in settori importanti[373]. E' insomma esatto che <<*[t]he more an owner, for his advantage, opens up his property for use by the public in general, the more do his rights become circumscribed by the statutory and constitutional rights of those who use it*>>[374]; pertanto è ora di chiedersi perché la violazioni <<*of the most basic values – speech, privacy and equality- should be tolerated just because the violator is a private enty rather than the government*>>[375].

98/6, 2020, 1142 ("*The state action doctrine is a complete mess. (..) The problem, though, is the line between state action and nonstate action is often nearly impossible to spot*") che sembra accennare alla possibilità di ravvisare anche una state action omissiva per non aver lo Stato rimosso ingiustizie e discrminazioni (sub II, p. 1146 ss e spt. p. 1154).

[370] Perel M.-Elkin-Koren N., *Accountability in algorithmic copyright enforcement*, cit., 488 (gli aa. segnalano che si inibisce il diritto di informare non solo attivo, ma anche passivo: pp. 483 e 491). <<*The Power to include, exclude, and rank is the power to ensure which public impressions become permanent and which remain fleeting*>> (Pasquale F., *The black box society*, cit., 61). Afferma l'insostituibilità e l'irrinunciabilità del servizio offerto da Facebook (nonché della sua essenzialità, parrebbe) Thobani S., *Il mercato dei dati personali*, cit., 143.

[371] Così Noah Harari Y., presentando il libro *Homo Deus. Breve storia del futuro*, secondo quanto riferisce Crisci S., *Intelligenza artificiale ed etica dell'algoritmo*, Il foro amm., 2018, 1787 ss., § 3.

[372] V. l'approfondito saggio di Cohen J. E., *Between truth and power*, cit., soprattutto a pp. 234-237.

[373] Ancora Cohen J. E., *Between truth and power*, cit., p. 240 ss sul ruolo centrale delle piattaforme nel flusso di informazioni di ogni tipo, che genera un'inusuale coinvolgimento (*entanglement*) publico-privato.

[374] Così la Corte Suprema USA in *Marsh v. Alabama* del 1946, primo caso in cui applicò la protezione del diritto di parola ad uno spazio privato (distribuzione di materiale religioso in una città privata, company town, cioè di proprietà di una corporation, da parte di un testimnone di Geova). Prendo la citazione da Peters J., *The "sovereigns of cyberspace" and state action: the first amendment's application—or lack thereof—to third–party platforms*, in *Berkeley technology law journal*, 2018, vol. 32/, 989 ss, a 1023.

[375] Anzi se lo chiedeva con queste parole nel 1985 il notevole saggio Chemerinsky E, *Rethinking State Action*, in *Northwesteren University law review*, Fall 1985, vol. 80/3, 503 ss. Qui trovi un'analitica critica all'inapplicabilità della

La natura formalmente privata degli enti de quibus non osta a riconoscere che il rischio ora proviene non solo dagli Stati (o dalla mano pubblica), ma anche –anzi in certi casi, proprio come per la libertà di espressione, assai di più- da poteri privati. Ne segue che le guarentigie, faticosamente ottenute verso gli Stati quando lì stavano i rischi per le libertà personali, ora vanno riconosciute già de iure condito pure verso le piattaforme, nella misura in cui detti rischi ora derivano da loro[376]. La valutazione,

State action doctrine agli enti privati: afferma anzi che, se lo scopo è proteggere la libertà individuale, è meglio abbandonarla (p. 550-551 e 554-555). *In nuce* è questa la ragione addotta da tutti coloro che affermano l'applicabilità del Primo Emendamento ai social network (da vedere per i motori di ricerca): ex multis v. Jackson B.F., *Censorship and Freedom of Expression in the Age of Facebook*, 44 New Mexico L. Rev. 121 (2014), passim, spt. sub B, p. 139 ss, e Williams A.M., *You Want to tweet about it but you probably can't: how social media platforms flagrantly violate the First Amendment*, in *Rutgers computer § technology law journal*, 2019, p. 106 ss, sub VII e VIII (è applicabile loro sia la *public function doctrine* che la *public forum doctrine*). L'invocabilità dei diritti costituzionali verso le maggiori corporations era stata già affermata da Adolf Berle jr. (l'autore assieme a G. Means del celeberrimo *The Modern Corporation and Private Property* del 1932) in *Constitutional limitations on corpoate activity-Protection of personal rights from invasion through economic power*, *Univ. of Penns. law review*, 1952, vol. 100/7, 933 ss, secondo cui la precondizione è che <<*the undeniable fact that the corporation was created by the state and the existence of sufficient economic power concentrated in this vehicle to invade the constitutional right of an individual to a material degree*>> (p. 943; l'a. attribuisce notevole importanza al ftto che la corporation sia <<a creature of the state>>). Berle, poi, a proposito del caso della company town in *Marsh v. Alabama* del 1946 (cit. sopra nella nota 373) si chiedeva cosa la rendesse <pubblica>, così rispondendo(-si): <<*The whim of a single houseowner directed towards his tenants' religious practices might be private. The prejudice of the owner of ninety per cent of the available housing would be a public matter.*>> (p. 953). In breve il problema all'inizio del 21° secolo è quello per cui <<*we have moved into a new kind of public sphere—a digital public sphere—without the connective tissue of the kinds of nstitutions necessary to safeguard the underlying values of free speech. We lack trusted digital institutions guided by publicregarding professional norms. Even worse, the digital companies that currently exist have contributed to the decline of other trusted institutions and professions for the creation and dissemination of knowledge…. Social media also need to become trusted mediating institutions guided by professional norms. They have to become trusted and trustworthy organizers and curators of public discourse. They aren't now*>> (Balkin, J. M., *How to Regulate (and Not Regulate) Social Media*, 15.03.2020, p. 9 e 10, in ssrn.com).

[376] La considerazione vale non solo per le piattaforme digitali, ma anche per qualunque altro ente privato, dotato di paragonabile capacità di influire sulla vita delle persone. Le prime, poi, nell'emergenza sanitaria da coronavirus, stanno andando sempre meglio in Borsa: R. Waters, *Big Tech is emerging from the crisis stronger than ever*, Financial Times, 22.05.2020. La preferenza per una

del se e da chi i diritti fondamentali siano lesi, va fatta in base al contesto storico-politico del momento in cui si pone la questione[377]: si tratta infatti non di schemi astratti, buoni per tutte le stagioni, ma da applicare in base alle circostanze. Osservò William Beveridge (l'autore del celebre Rapporto Beveridge nel Regno Unito): <<*libertà non vuol dire soltanto essere al riparo dagli arbitrii governativi, ma vuol dire anche affrancamento dalla servitù economica derivante dall'indigenza, dalla miseria e da altri mali sociali; vuol dire libertà dai poteri arbitrari sotto qualsiasi aspetto. Un uomo che muore di fame non è libero; perché fino a che non si sa nutrito, egli non può avere altro pensiero che quello di soddisfare le sue necessità fisiche, e pertanto da uomo è ridotto in animale. Un uomo che non osa ribellarsi contro ciò che egli sente come un'ingiustizia inflittagli dal suo datore di lavoro o dal suo dirigente, per paura che questo lo condanni alla disoccupazione cronica, non è libero*>>[378].

La dottrina inizia a muoversi in questo senso[379], per cui è

conoscenza distribuita, invece che accentrata, sostenuta a suo tempo da Hayek nei confronti dello Stato, oggi va fatta valere verso i colossi informatici e finanziari, in particolare per la segretezza dei loro processi decisionali (così Pasquale F., *The black box society*, cit., p. 214). Sulla stessa lunghezza d'onda di quanto osservato nel testo è Betzu M., *Libertà di espressione e poteri privati nel cyberspazio*, in *Diritto costituzionale*, 2020/1, 119 e 130-131.

[377] Ciò è stato anche precisato (Mostacci E., *Critica della ragione algoritmica*, cit., 69-70), ma si tratta di un'ovvietà: il diritto (qualunque sua branca) è governo di relazioni umane, non esercizio di una qualche logica astratta, per cui è impensabile applicarlo prescindendo dai condizionameni storico-sociali (di questo a. si v. l'interessante § finale, che sintetizza il suo pensiero circa ll'influenza di internet sui processi democratici, p. 127 ss).

[378] Beveridge W., *Perché sono liberale*, del 1947, prima parte letta in Acemoglu D.-Robinson J.A., *La strettoia. Come le nazioni possono essere libere*, cit., 659, mentre l'intero passaggio si trova in rete (ad es. in *Non mollare*, n. 62, 20 aprile 2020, criticaliberale.it). Esamina l'evoluzione della giurisprudenza della Corte Suprema dalla dottrina *Lochner* (si parla di *lochnerism* da una celebre sentenza Lochner v. New York del 1905 per indicare un attegiamento della Corte astensivo, in formalistico rispetto di presunte autonomie private) ad alcune aperture successive -ma limitate ratione materiae- che valorizzano la situazione reale, Laker G., *The First Amendment's reale Lochner problem*, in *The University of Chicvago law review*, vol. 87/5, 2020, sub III, p. 1300 ss.

[379] Oltre ai saggi già indicati (spt. in nota 364) e mescolando dottrina italiana e straniera, v. ad es.: Ainis M., *Il regno dell'uroboro*, cit., 65- 66 (secondo cui la dottrina del *public forum* dovrebbe valere pure per Internet); Everett C. M., *Free Speech on Privately-Owned Fora: A Discussion on Speech Freedoms and Policy for Social Media*, *Kansas Journal of law and public policy*, vol. 28/1, 113 ss (con

toni decisi, affermando che si tratta di *state action* dato che Facebook, quando censura, non fa che applicare una legge statale -§ 230 CDA- che incentiva la censura stessa: p. 139 ss); Geddes K., *Meet Your New Overlords: How Digital Platforms Develop and Sustain Technofeudalism*, cit., p. 465-469 (anche perché la rimozione è incoraggiata dallo Stato tramite il § 512 DMCA, per cui l'estensione della State action doctrine è giustificata); - Fischman Afori O., *Online Rulers as Hybrid Bodies: The Case of Infringing Content Monitoring (April 15, 2020)*, in *University of Pennsylvania Journal of Constitutional Law*, Forthcoming, leggibile in ssrn.com, sub V, p. 34 ss, applicando la teoria degli *hybrid (public/private) bodies*, secondo cui anche gli enti privati che esercitanjo pubbliche funzioni devono rispettare i diritti fondamentali (sub IV.D); - Golia A. Jr., *L'antifascismo della Costituzione italiana alla prova degli spazi giuridici digitali. Considerazioni su partecipazione politica, libertà d'espressione online e democrazia (non) protetta in CasaPound c. Facebook e Forza Nuova c. Facebook*, in *federalismi.it*, n. 2020/18, p. 180, p. 144-145; Hudson D.L., *In the Age of Social Media, Expand the Reach of the First Amendment*, in *Human rights magazine*, vol. 43/4, ottobre 2018, American Bar Association, passim; Peters J., *The "sovereigns of cyberspace" and state action*, cit., 1023-1024; Patty M., *Social Media and Censorship: Rethinking State Action Once Again*, in *Mitchell Hamline Law Journal of Public Policy and Practice*, 2019, Vol. 40, 98 ss, 114-115 e 126; Yemini M., *Missing in "state action": toward a pluralist conception of the first amendment*, in *Lewis & Clark Law review*, 2020, vol. 23/4, 1149 ss, passim (spt. sub II, 1163 ss, e sub IV.A e IV.C, 1195 ss); Monti M., *La disinformazione online, la crisi del rapporto pubblico esperti e il rischio della privatizzazione della censura nelle azioni dell'Unione Europea (Code of practice on disinformation)*, in Federalismi, 2020/11, 24.04.2020, leggibile in federalismi.it, 304 (apprezzando le tesi di Klonick K. e Peters J., citt sopra); Bailey K.C., *Regulating ISPs in the Age of Technology Exceptionalism*, in *Texas law review*, 2020, vol. 98/5, 953 ss, pp. 960-964, sub III, basandosi sull'insgnamento del *technology exceptionalism* addotto dalla Corte Suprema in *Riley v. California* (2014) e in *Carpenter v. United States* (2018) sull'appplicabilità del Quarto Emendamento al sequestro dei telefoni cellulari (l'a. però ritiene allo stato improbabile analoga apertura agli ISPs: p. 964); Geddes K., *Meet Your New Overlords: How Digital Platforms Develop and Sustain Technofeudalism*, cit., 463-469 passim (centrato sul copyright, approfondendo tre effetti negativi della rimozione automatica tramite Content-ID di Youtube: i) rimozione di contenuti leciti a causa di falsi positivi, ii) erosione degli usi leciti soprattutto in base al fair use, iii) conseguentemente al punto precedente, sfruttametno non retribuito del lavoro degli utenti erroneamente "rimossi" tramite la monetizzazione –appunto erroneamente- proposta ai copyright holders); Marique Y.-Marique E., *Sanctions on Digital Platforms: Balancing Proportionality in a Modern Public Square*, in *Computer Law & Security Review*, 2019, 1 ss., §§ 2-3 (forse, dato che scrivono di *modern public square*, pur non traendone conseguenza in tema di rispetto della libertà di espressione, e di dovere di creare *sanctions* e rispettare la *proportionality*, anche se non è chiaro se come doveri pubblicistici o solo per evitare responsabilità civili); sostanzialmente anche Kerr R.L., *From Holmes to Zuckerberg*, cit., 480-1, 497-502 e 511 (suggerendo larga applicazione del Primo Emendamento per continuare a favorire il c.d. *marketplace of ideas*); Whitney H., *Search Engines, Social Media, and the Editorial Analogy*, cit., 136-141, evidenziando la somiglianza con uno *shopping mall* o comunque *public forum* (ma pure il rischio che ciò comporterebbe un abbandono di massa dei social, p. 143); Zicchittu P., *La*

possibile un futuro adeguamento anche giurisprudenziale: possibile ma non probabile, dato che non mancano opinioni contrarie[380]. In ambiente common law si discorre di digital due

libertà di espressione dei partiti politici nello spazio pubblico digitale: alcuni spunti di attualità, in *Riv. dir. dei media*, medialaws.eu, 09.04.2020, § 5 (annotando le due ordinanze romane a cavallo tra il 2019 e il 2020 relative alle liti tra, da una parte, Facebook e, dall'altra, CasaPound in una e Forza Nuova nell'altra); Zecca D., *Soluzioni tradizionali per piattaforme moderne: la state action (non) mostra i segni del tempo*, nota a US Corte d'appello Nono circuito, 26 febbraio 2020, *Prager University, v. Google and YouTube* del 2020, cit., in medialaws.eu, 05.05.2020, § 3, qualificando le decisioni censorie delle piattaforme come attività delegata dallo Stato, secondo la teoria statunitense della *collateral censorship*: posizione però di dubbia esattezza, non essendo in realtà ravvisabile tale delega né formale né informale, fattuale, dato che la decisione della piattaforma può essere sempre impugnata giudizialmente e che si tratta di spazi formalmente privati (per cui forse di delega si può parlare solo intendendola in senso sociopolitico come momentanea scelta statale di non intervenire in via regolatoria e sempre salva l'azione in corte; scrivono di scelta degli Stati di affidarsi alle piattaforme per l'applicazione delle rispettive leggi Marique E.-Marique Y., *Sanctions on digital platforms: beyond the public–private divide*, in *Cambr. intern. law jour.*, 2019, v ol. 8/2, 258 ss, § 2.1, p. 260, ma in accezione poco chiara, dato che alla fine osservano <<*private actors behave as the 'armed face' of the public authorities in the digital space, to avoid being themselves sanctioned in the physical world.*>>, p. 263-4, il che sembra altro dalla scelta statale di affidarsi alle piattaforme) (la scelta di collaborazione tra pubblico e privato fa però parte della storia polico-sociale degli Stati Uniti: Acemoglu D.-Robinson J.A., *La strettoia. Come le nazioni possono essere libere*, cit., cap. 10, p. 411 ss., spt. 427 ss, che scrivono di "partenariato" a tale proposito); Ferrajoli L.,*Manifesto per l'uguaglianza*, Laterza, 2018, p. 258-261 (sul costituzionalismo da estendere ai poteri extra- o sovra-statali, a quelli economico-privati in primis). V. pure Chemerinsky E, *Rethinking State Action*, cit.: la ragione storica dell'accezione restrittive di <state Action> sta nel fatto che all'epoca di stesura della Costituzione si riteneva che la common law proteggesse a sufficienza dalle intrusioni provenienti da soggetti privati (p. 511-519, passim).

[380] Ad es.: - Bridy A., *Leveraging CDA 230 to Counter Online Extremism*, *George Washington University Program on Extremism Legal Perspectives on Tech Series*, 2019, in ssrn.com, p. 6/7; Gillespie T., *Custodians of the internet*, cit., p. 176/7 (che ricorda l'alternativa del nacondere il post, praticata ad es. da Tumblr: 177 ss e 182 ss., *hiding tactics*);- Conroy A., *The First Amendment's Role on the Internet Governed by Private Actors*, cit., p. 387/8 soprattutto perchè (p. 394) violerebbe il diritto delle stesse piattaforme di invocare per sé il Primo Emendamento (meglio qualificabile però come libertà di impresa anzichè libertà di espressione, almeno da noi); - Franks M.A., *The Free Speech Black Hole: Can The Internet Escape the Gravitational Pull of the First Amendment?*, in *Knight First Amendment Institute-Columbia University, knightcolumbia.org*, 21 agosto 2019 (saggio interessante e per molti versi condivisibile); - Grafanaki S., *Platforms, the First Amendment and Online Speech: Regulating the Filters*, cit., passim, lavoro interessante, il cui concetto centrale è la distinzione tra servizi di hosting e servizi utili alla navigazione (in pratica: algoritmi per newsfeed e per elenco risultati nei motori di ricerca), p. 117-8: l'a. esonera i primi da

regolamentazione per la loro incomprimibile autonomia simil-editoriale (p. 136, 138, 140; ma allora anche gravati da responsabilità editoriale!) e ammette invece l'assoggettabilità dei secondi ad una qualche regolamentazione (sub II.B, pp.141-151) per giungere ad escludere i newsfeed personalizzati –come tutti ormai, credo- che in quanto tali fuoriescono dal concetto di *public discourse* e dunque da ogni tutela ex Primo Emendamento, p. 151 ss); -Hooker M., *Censorship, Free Speech & Facebook: Applying the First Amendment to Social Media Platforms via the Public Function Exception*, in Washington Journal of Law, Technology & Arts, Vol. 15/1, 2019, 36 ss., sub IV.A, 60 ss (perché la conduzione dei social non è *public function* nel senso –di *uniquely public*- adottato dalla giurusprudenza statunitense: ma da noi con l'analogia iuris o legis tale ostacolo potrebbe essere superato) leggibile in ssrn.com ; - Jaffe A.G., *Digital shopping malls and state constitutions — a new font of free speech rights?*, in *Harvard Journal of Law & Technology*, Vol. 33/1, 2019, 270 e 280-3, per l'insuperabile ostacolo posto dal § 230 Decency Act; Karanicolas, M., *Squaring the Circle Between Freedom of Expression and Platform Law*, cit., 199-200; Klonick K. in *The New Governors*, cit., 1658 ss (né *state actors* né editori ma, semmai, *broadcasters* o *public utilities/common carriers*) e in *The Facebook Oversight Board*, cit., 2428; - Kadri T.E.-Klonick K., *Facebook v. Sullivan*, cit., 71 (<<Even though Facebook need not adhere to the First Amendment, its content-moderation policies were largely developed by American lawyers trained and acculturated in American free-speech norms....>>) e 94 (le piattaforme sono in sostanza editori, visto che <<act as editorial boards determining what types of content see the light of day>>); - Minow M., *Alternatives to the State Action Doctrine in the Era of Privatization, Mandatory Arbitration, and the Internet: Directing Law to Serve Human Needs*, in *Harvard Civil Rights-Civil Liberties Law Review*, 2017, vol. 52/1, 157; - Suzor N.P., *Lawless. The secret rules that govern our digital lives*, cit., p. 8/11 (pur riconoscendo che la platform governance è di rilievo costituzionale, su cui v. pure cap. 8 e 9 a p. 105 ss e risp. 115 ss, non chè p. 165-167); - Sunstein C., *Twitter Strikes Fair Balance Between Liberty and Lies*, 27.05.2020, Bloomberg Opinion, in bloomberg.com, a proposito dell'etichetta "*contain potentially misleading information about voting processes and have been labeled to provide additional context around mail-in ballots*", apposta da Twitter ad un tweet del presidente Trump, il quale ha minacciato l'emissione di un *executive order* per ridurre il safe harbour nel senso di considerare il "selective censoring" come violazione del diritto al free sprech (secondo la bozza vista dai giornalisti: così Haberman M.-Conger K., *Trump Prepares Order to Limit Social Media Companies' Protections*, *The New York Times*, 28 maggio 2020, edizione online, e Baker P.-Wakabayashi D., *Trump's Order on Social Media Could Harm One Person in Particular: Donald Trump*, *The New York Times*, 28 maggio 2020, edizione online), con scelta definita <<ironica>> dall'Editorial Board *Fact-checking Donald Trump's Twitter feed. Social media sites should clamp down on misinformation* del Finanzial Times del 28 maggio; - Citron D.K.—Franks M.A., *The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform, Boston University School of Law Public Law & Legal Theory Paper No. 20-8*, gennaio 2020, sub II.B, p. 14 ss. Secondo le aa., anche se si applicasse alle piattaforme la *state action doctrine*, non si potrebbe più applicar loro la disciplina del Buon Samaritano ex § 230 *Communications Decency Act* del 1996 – title 47 U.S. Code (Citron D.K.—Franks M.A., cit., p. 18): ciò perché <<*if platforms like Facebook or Twitter were treated as quasi-governmental actors, they could not act as "Good Samaritans" to block the assaults of cyber mobs, as contemplated by the drafters of the*

process[381] oppure di information fiduciaries[382] in relazione alle c.d. media companies (posizione quest'ultima ora

Communications Decency Act of 1996.120 They could not protect against spam, doxxing, or impersonations. There is good in having private platforms wield some bounded power to address online abuse and other activity that imperils free expression.>> (Citron D.K.-Richards N.M., *Four principles for digital expression (you won't believe #3!)*, in *Washington university law review*, vol. 95, 2018, 1371); - similmente Hooker M., *Censorship, Free Speech & Facebook*, cit. sopa in questa nota, 56/7 (che aggiunge la indesiderata conseguenza della impossibilità di lasciare ai singoli di bloccare i post fastidiosi, p. 63: il che però non è, mi pare, dato che questo da un lato è scelta del singolo e dall'altro avverrebbe solo per i personaggi pubblici); - Thai J., *Facebook's Speech Code and Policies*, cit., 1644, pur evidenziando che i *Community Standards* di Facebook sono lontani dal permettere il *free speech* che l'azienda proclama (sub I.B, 1650 ss), tranne che – notoriamente- per i politici (l'a. osserva poi che Donald Trump nella campagna elettorale 2020 è al momento *the platform's top spender on political ads*: p. 1686); - Wu T., *Is the First Amendment Obsolete?*, Michigan Law Review, 2018, vol. 117, p. 547 ss a p. 22-23, per la difficoltà di discriminare le fonti di potere soverchiante, a cui imporre il Primo Emendamento, dalle altre (non è così: vi rientrano tutte quelle di rilevante interesse collettivo, certo con un'inevitabile vaghezza determinativa) e per l'inconveniente che verrebbe limitata la capacità della piattaforma di combattere spamming, trolling, flooding, e simili abusi (non capisco perché: anche l'ente che svolga funzione pubblica ha il potere/dovere di impedire fatti -anche solo potenzialmente- illeciti nella sfera da lui controllata). Si tratta comunque di tema complesso, soprattutto circa il *false speech* (su cui Chemerinsky E., *False speech and the First Amendment*, in *Oklahoma law review*, 2018, vo. 71/1, p. 1 ss). Ci sarebbe effettivamente un conflitto apparente: dover permettere il diritto di parola può sembrare a prima vista inconciliabile con il safe harbour per rimozione/disabilitazione. Solo in apparenza, però, dato che: i) il safe harbour esenta solo da responsabilità civile e non da inibitorie (come nel safe harbour europeo); ii) comunque il provider conserva il diritto di rimuovere tutto ciò la cui conservazione può costituire da parte sua illecito giuridico di qualunque tipo; iii) sempre che sia costituzionalmente legittima una disposizione così vaga come <<material … otherwise objectionable>> per indicare i materiali che il provider può liberamente rimuovere (§ 230 CDA sub c.2.A). In ogni caso da noi una simile disposizione non c'è e comunque in generale una tale pretesa -basata sul diritto di parola- verso le piattaforme non può elidere il diritto/onere di queste di impedire materiali illeciti e cioè di quelli il cui hosting può comportare per esse responsabilità di qualche tipo (nel diritto statunitense, poi, si è anche fatto notare che il divieto di censurare arbitrariamente non costituisce *compelled speech* vietato, visto che le posizioni dell'utente uploader e della piattaforma rimerrebbero ben distinte: Everett C. M., *Free Speech on Privately-Owned Fora*, cit. alla nota 378).

[381] Mostert F., *"Digital due process": a need for online justice*, marzo 2020, di prossima pubblicazione in *Journal of Intellectual Property Law & Practice,* letto in ssrn.com, spt. p. 13 ss.; Van Loo R., *Federal rules of platform procedure*, cit., sub III.B-D, pp. 28-45, passim.

[382] Balkin J.M.-Zittrain J., *A Grand Bargain to Make Tech Companies Trustworthy*, in The Atlantic, 03.10.2016, con riferimento alla privacy.

convincentemente criticata, dato che, in presenza di frontale conflitto di interessi, è illogico e controproducente limitarsi a gravare le piattaforme di un vago legame fiduciario sulla falsariga di quello gravante su avvocati medici e notai[383]). Addirittura si osserva[384] che l'approccio tradizionale, fondato sull'invocazione del Primo Emendamento come diritto assoluto e incomprimibile (*posts as trumps*, adattando l'espressione di Dworkin *rights as trumps*) è individualistico, limitante e superato, dovendo caratterizzarsi invece per la *proportionality* (bilanciamento sistematico tra interessi confliggenti)[385] e la *probability* (considerazione del tasso di errori che la piattaforma

[383] La cennata critica è portata dall'interessante lavoro di Khan L.M.-Pozen D.E., *A Skeptical View of Information Fiduciaries*, cit., passim (Zuckerberg, non stranamente, ha mostrato interesse per la proposta di Balkin-Zittrain: Khan L.M.-Pozen D.E., op. cit., p. 501, testo e nota 12). Infatti chiedere il rispetto della privacy alle piattaforme è come chiedere a Henry Ford di costruire ogni Model T a mano (così Srnicek N., *Capitalismo digitale*, cit., p. 87, citando Zuboff). Da noi, norme come l'art. 21 TUF (obbligo di servire al meglio l'interesse del cliente; da vedere se era realmente necessaria per arrivare al medesimo risultato, se non per la –oggi indiscutibile- inderogabilità in peius) fanno diventare attività "finalizzata" quella dell'intermediario finanziario, al punto che si parla al proposito di ufficio di diritto privato (così Di Raimo R., *Ufficio di diritto privto e carattere delle parti professionali quali criteri ordinanti delle negoziaioni bancaria e finanziaria (e assicurativa)* in *Giust. civ.*, 2020/2, p. 320 ss e spt. § 6 a p. 335 ss).

[384] E' il centro del saggio di Douek E., *Governing Online Speech: From 'Posts-As-Trumps'*, cit. (la quale però non riesce a liberarsi del dogma, per cui il Primo Emendamento non si applica alle piattaforme in quanto enti privati: p. 10). L'a. osserva che con la pandemia del 2020 il ruolo della *human moderation* è scemato ed aumentato invece quello algoritmico (p. 36): conf. Magalhães J.C.-Katzenbach C., *Coronavirus and the frailness of platform governance*, in *Internet policy review*, 29 marzo 2020, *policyreview.info* (fenomeno abbastanza prevedibile, del resto). Il legame tra piattaforme, content moderation e A.I. è autorinforzantesi: le piattaforme hanno ormai raggiunto un volume di dati da gestire per cui solo l'A.I. può provvedervi, ma, al tempo stesso, il ricorso all'A.I. permette alle piattaforme di diventare sempre più grandi (Gillespie T., *Content moderation, AI, and the question of scale*, *Big Data & Society*, 2020/2, p. 2).

[385] Douek E., *Governing Online Speech: From 'Posts-As-Trumps'*, cit., p. 10 ss. e 34. La tecnica del bilanciamento tra interessi confliggenti, che forse spaventa la tradizione USA sostenitrice della primazia del diritto di parola (l'a. spende pagine per difenderlo: p. 46 ss, sub III), da noi costituisce invece "moneta corrente", essendo da lungo tempo teorizzata dagli aa. e applicata dai giudici: v. ad es., per restare al diritto costituzionale, Morrone A., voce *Bilanciamento (giustizia cost.)*, in *Enc. dir., Annali II-2*, Giuffrè, 2008, p. 185 ss, e Celotto A., voce *Diritti (diritto costituzionale)*, *Digesto- dir. pubbl.*, 2017, § 13 (letto in Pluris on line).

può fare, entro certi limiti inevitabili e dunque da accettare)[386]: anche se si tratta di posizione legata alla preminenza statunitense del diritto di parola (che forse sta dunque cambiando), da noi invece abbastanza pacifica, essendo agevolmente inquadrabile con il ricorso a principi o norme costituzionali, da un lato, e con la diligenza (tecnica), dall'altro. Infatti nel nostro ordinamento, visto che intercorre rapporto contrattuale tra l'utente e la piattaforma, già un buon passo sarebbe valorizzare la buona fede in executivis, opportunamente modulandola per tener conto dell'enorme disparità di potere contrattuale e cognitivo tra i contraenti, almeno quanto alla tutela individuale.

Il problema sorge proprio in relazione a quest'ultima circostanza, dato che la tutela individuale sarà assai raramente azionata in sede contenziosa. Si potrebbe anche pensare –alla luce ad es. del ruolo informativo fondamentale svolto dalle piattaforme in occasione della gravissima emergenza sanitaria, che ha colto il mondo intero all'inizio dell'anno 2020- ad una qualificazione come public utility (digitale), seppur de facto invece che de iure.

Qualche timido passo di consapevolezza è stato intrapreso a livello europeo modificando la disciplina dei servizi di media audiovisivi[387]. Solo che le interessanti considerazioni astratte sul ruolo dei social media (cons. 4-5 della dir. 2018/1808) hanno poi portato alla scelta di normare solo le piattaforme di condivisione

[386] Douek E., *Governing Online Speech: From 'Posts-As-Trumps'*, cit., p. 25 ss. Simile impostazione (seppur in un'ottica generale) in Zittrain J., *Three Eras of Digital Governance*, 2019, disponibile in *ssrn.com*: "*We have moved from a discourse around rights – particularly those of end-users, and the ways in which abstention by intermediaries is important to facilitate citizen flourishing – to one of public health, which naturally asks for a weighing of the systemic benefits or harms of a technology, and to think about what systemic interventions might curtail its apparent excesses*".

[387] Dir. UE 2018/1808 del 14.11.2018, che modifica la dir. UE 2010/13/E (direttiva sui servizi di media audiovisivi). Altro importante tema è quello della equiparabilità della comunicazione politica tramite social a quella tradizinale oggetto di legislazione ad hoc, soprattutto in tema di campagne elettorali (par condicio, divieto di diffusione di sondaggi nei giorni precedenti, etc.). Anche optando per una disciplina ad hoc, non mancherebbero le difficoltà tecniche: v. Meola F., *Tecnologie digitali e neuro-marketing elettorale. A proposito di una possibile regolamentazione delle nuove forme di propaganda politica*, in *costituzionalismo.it*, 2020/1, p. 118 ss e 124 ss.

video[388], pur affermandosi che la libertà di espressione è <<fondamento dei sistemi democratici>>[389].

21. (segue): recenti provvedimenti giurisdizionali italiani sul tema

La tesi qui sostenuta è affermata da un provvedimento italiano cautelare del 2019, che ha ordinato a Facebook la riattivazione di una pagina illegittimamente disattivata. La motivazione richiederebbe maggior approfondimento, per cui mi limito a riportare il passo più pertinente al discorso qui svolto[390]: <<*È infatti evidente il rilievo preminente assunto dal servizio di Facebook (o di altri social network ad esso collegati) con riferimento all'attuazione di principi cardine essenziali dell'ordinamento come quello del pluralismo dei partiti politici (49 Cost.), al punto che il soggetto che non è presente su Facebook è di fatto escluso (o fortemente limitato) dal dibattito politico italiano, come testimoniato dal fatto che la quasi totalità degli esponenti politici italiani quotidianamente affida alla propria pagina Facebook i messaggi politici e la diffusione delle idee del proprio movimento. Ne deriva che il rapporto tra Facebook e l'utente che intenda registrarsi al servizio (o con l'utente già abilitato al servizio come nel caso in esame) non è assimilabile al rapporto tra due soggetti privati qualsiasi in quanto una delle parti, appunto Facebook, ricopre una speciale posizione: tale speciale posizione comporta che Facebook, nella contrattazione con gli utenti, debba strettamente attenersi al rispetto dei principi costituzionali e ordinamentali finché non si*

[388] La dir. UE 2018/1808, tra le varie modifiche alla dir. UE 2010/13/E, ha inserito il capo IX bis sulle piattaforme di condivisione video (cioè artt. 28 bis-28 ter). Si prenda il cons. 4 della dir. 2018/1808: dopo aver equiparato i "servizi dei media sociali" ai "servizi di piattaforma per la condivisione di video" (primi quattro periodi), inspiegabilmente conclude: "*di conseguenza (..) tali servizi dovrebbero essere disciplinati dalla direttiva 2010/13/UE nella misura in cui rispondono alla definizione di servizio di piattaforma per la condivisione di video*". Non è chiaro il nesso di conseguenqualità (rectius: pare esservi incoerenza) tra l'equiparazione iniziale e la limitazione finale alle sole piattaforme di condivisione video (anche perché pure in tutti i social si possono caricare audiovisivi).

[389] Lo fa notare Manetti M., *Regolare internet*, in *Riv. dir. dei media*, 2020, www.medialaws.eu, p. 12.

[390] Forse un po' lungo, ma ne vale la pena, data l'importanza del comando impartito.

dimostri (con accertamento da compiere attraverso una fase a cognizione piena) la loro violazione da parte dell'utente. Il rispetto dei principi costituzionali e ordinamentali costituisce per il soggetto Facebook ad un tempo condizione e limite nel rapporto con gli utenti che chiedano l'accesso al proprio servizio. Conseguentemente ai principi sopra esposti, l'esclusione dei ricorrenti da Facebook si pone in contrasto con il diritto al pluralismo di cui si è detto, eliminando o fortemente comprimendo la possibilità per l'Associazione ricorrente, attiva nel panorama politico italiano dal 2009, di esprimere i propri messaggi politici>>[391]. Il successivo reclamo cautelare ha confermato la decisione, affermando sul punto specifico l'applicabilità diretta dei precetti costituzionali nella disciplina del rapporto contrattuale[392]: <<*In generale si deve ritenere preclusa all'autonomia privata la limitazione a carico di uno dei contraenti dell'esercizio di diritti costituzionalmente garantiti, attuata ricollegando al loro esercizio conseguenze negative sul piano contrattuale, tanto più in assenza di una giustificazione oggettiva nella funzione riconosciuta al contratto*>> (§ 8) e <<*Al contrario se la posizione del gestore è riconducibile alla libertà di impresa tutelata dall'art. 41 della Costituzione, quella dell'utente è riconducibile, di fronte a contestazioni relative alle opinioni espresse sulla piattaforma, alla libertà di manifestazione del pensiero protetta dall'art. 21 e, di fronte a contestazioni relative alla natura ed agli scopi dell'associazione, all'art. 18 e quindi a valori che nella gerarchia costituzionale si collocano sicuramente ad un livello superiore. Si deve concludere che la disciplina contrattuale non*

[391] Si tratta di Trib. Roma, 11.12.2019, *CasaPound Italia c. Facebook*, leggibile ad es. in *Dir. informaz. informat.*, 2020, 104 ss. Il provvedimento è qui annotato da B. Mazzolai, *La censura su piattaforme digitali: il caso Casa Pound c. Facebook*, che ipotizza (pp. 116-117) tre qualificazioni possibili per le piattaforme: associazioni private ex art. 2 Cost.; mezzi di comunicazione, con obbligo di par condicio in ambito informativo; luoghi aperti al pubblico ex art. 17 Cost. L'a. ne ipotizza, per vero, anche una quarta (*public forum*, secondo il diritto statunitense): la quale però, non avendo autonomia concettuale per disomogeneità rispetto alle precedenti (ordinamento diverso), sarà più proficuo ricondurla alle categorie costituzionali nazionali. Commento positivo (e negativo per quella relativa a Forza Nuova) pure da parte di Caruso C., *I custodi di silicio. Protezione della democrazia e libertà d'espressione nell'era dei social network*, in Consulta OnLine, *Liber amicorum per Pasquale Costanzo*, 17.03.2020, § 4.

[392] Trib. Roma, deciso il 29.04.2020, RG 80961/19, *Facebook v. CasaPound*, al momento pubblicata dal Corriere della Sera.

può lecitamente assumere quale causa di risoluzione del rapporto manifestazioni del pensiero protette dall'art. 21 né consentire l'esclusione di associazioni tutelate dall'art. 18>> (§ 10). Non entro nel merito dell'appropriatezza del giudizio nel caso specifico; mi limito a segnalare la regola astratta, innovativa anche se bisognosa di qualche approfondimento[393].

[393] Ad esempio circa: - l'individuazione di quali enti privati sottostiano all'applicabilità diretta delle disposizioni costituzionali (tutte o solo le maggiori), anche in presenza di eventuali clausole contrastanti; - l'individuazione di quali diritti costitizionali siano così azionabili, - la disposizione costituzionale azionata, dato che il primo grado cautelare applica la tutela del pluralismo politico e specificamente il diritto di associazione partitica ex art. 49, mentre il reclamo applica il diritto di manfestare il proprio pensiero (art. 21) e quello di associazione generale (art. 18). Il che fa sorgere dubbi processuali, dato che il reclamo è sì impugnazione di tipo devolutivo ma per alcuni entro i limiti della prospettazione del reclamante (Corsini F., *Il reclamo cautelare*, Giappichelli, 2020, p. 108 ss, che però è a favore dell'effetto devolutivo automatico pieno ed assoluto; nello stesso senso Rescio N., *Note sull'impiego del reclamo (in luogo dell'appello) come mezzo per impugnare le sentenze con devoluzione automatica piena*, in *Riv. dir. proc*., 2008, pp. 966/7, che adduce nello stesso senso anche C. Cost. 65/1998) e del resto il principio *jura novit curia* è dubbio permetta di applicare indifferentemente gli articoli citati (forse si, per gli artt. 18 e 49: ma dipenderà dalla prospettazione iniziale del ricorrente). Lascia perplessi la critica dell'invocazione dell'art. 49 Cost., perché CasaPound non potrebbe essere un partito (e quindi invocare l'art. 49 Cost.), dato che la legge 383 del 07.12.2000 sulle associazioni di promozione sociale (quale pare sia CasaPound) lo vieterebbe (Quarta A., *Disattivazione della pagina Facebook. Il caso CasPound tra diritto dei contratti e bilanciamento dei diritti*, in *Danno e resp.*, 2020/4, 491/2, nota molto critica al provvedimento; l'a. esclude la invocabilità della teoria del *public forum* in Italia, p. 493). Se tale impedimento è quello costituito dall'art. 2 c.2 della cit. legge (<<*Non sono considerate associazioni di promozione sociale, ai fini e per gli effetti della presente legge, i partiti politici, le organizzazioni sindacali, le associazioni dei datori di lavoro, le associazioni professionali e di categoria e tutte le associazioni che hanno come finalita' la tutela esclusiva di interessi economici degli associati*>>), la critica non è centrata. Da un lato, l'esclusione è ai soli effetti della citata legge. Dall'altro, la disposizione è stata abrogata dal codice del terzo settore d. lgs. 3 luglio 2017 n. 117 art. 102 c.1 lett. a); né la nuova disciplina delle associazioni di promozione sociale, qui contenuta, parrebbe prevedere analogo divieto, nemmeno ai limitati fini del codice stesso, visto che la disposizione (verosimilmente) corrispondente (art. 35 c.2, d. lgs. 117/2017), recita: <<*Non sono associazioni di promozione sociale i circoli privati e le associazioni comunque denominate che dispongono limitazioni con riferimento alle condizioni economiche e discriminazioni di qualsiasi natura in relazione all'ammissione degli associati o prevedono il diritto di trasferimento, a qualsiasi titolo, della quota associativa o che, infine, collegano, in qualsiasi forma, la partecipazione sociale alla titolarita' di azioni o quote di natura patrimoniale*>>. Ci sarebbe piuttosto da interpretare il concetto di "partito", emergente dall'art. 49 Cost. (soprattutto le sue necessarie finalità "generali"), per verficare se comprende le <<attivita' di interesse generale per il perseguimento, senza scopo di lucro, di

In senso contrario si è osservato che affermare estesi doveri di permettere l'accesso, presupporrebbe ritenere la piattaforma "servizio pubblico", in mancanza di norma in tale senso[394]. L'obiezione è seria, solo che l'autore mi pare non consideri a sufficienza la via dell'applicazione diretta della tutela costituzionale della libertà di espressione: in particolare della sua applicazione ad un ambiente sì privato, ma che è diventato imprescindibile per la comunicazione pubblica. Per dare attuazione a detta tutela bisogna attendere norma ad hoc oppure si può pensare ad un'applicabilità immediata? Il punto è questo, più che quello dell'applicabilità pretoria della disciplina da presunto servizio pubblico. Il problema dell'applicabilità immediata dei principi costituzionali nei rapporti privatistici patrimoniali è ampiamente trattato: la risposta da dare è in generale negativa[395], a meno che ricorra la lesione di diritti fondamentali[396].

Ad analogo esito cautelare è giunta la Corte Costituzionale tedesca sempre in una lite tra un partito di destra e Facebook, al quale ha ordinato di riattivare il profilo: anche se il provvedimento pare motivato solo quanto al periculum in mora,

finalita' civiche, solidaristiche e di utilita' sociale>> di cui all'art. 5 c.1 (richiamato dall'art. 35 c.1) del d. lgs. 117/2017): la risposta potrebbe forse anche essere positiva (si v. l'elenco –con valore solo esemplificativo, direi- presente nel medesimo art. 5 c. 1; e sempre che rilevino le attività declamate, invece di quelle in concreto poste in essere, nel caso di divergenza tra le due) (esame dei caratteri distintivi dell'associazione partito politico in Rizzoni G., Art. 49, in *Comm. alla Cost.* dir. da Bifulco-Celotto-Olivetti, Utet, 2006, 1, sub § 2.3., p. 985/6).

[394] Falletta P., *Controlli e responsabilità dei social network sui discorsi d'odio online, Riv. dir. dei media*, medialaws.eu, 156-157.

[395] Tranne i canali di ingresso previsti dall'ordinamento e cioè essenzialmente tramite le clausole generali e l'interpretazione conforme a Costituzione.

[396] Simile la conclusione dell'approfondito lavoro di Golia A. Jr., *L'antifascismo della Costituzione italiana alla prova degli spazi giuridici digitali*, cit., p. 179/180, che ammette l'applicazione della policy di Facebook tranne quando è incompatibile con i valori costituzionali del singolo Stato. L'a. approva sostanzialmente l'ordinanza 11.12.2019 *Facebook v. CasaPound*, ravvisandovi un'applicazione non dichiarata della *unmittelbare Drittwirkung* (effetto orizzontale diretto dei diritti costituzionali: p. 1578 e 171), anche se ne rileva due limiti (oltre al fatto che non menziona l'art. 21 Cost, ma solo l'art. 49): l'efficacia pratica assai ridotta (ma questo non è addebitabile al giudice!) e la eccessiva tolleranza verso movimenti estremisti, che rischia di risolversi in una forma di autolesionismo costituzionale (p. 173-174).

stimato in base ad un bilanciamento dei contrapposti pericula[397].

In un caso simile[398] e di poco seguente, il Tribunale romano è invece giunto a conclusione opposta: si tratta dell'ordinanza 23.02.2020 nel caso Forza Nuova (rectius: attivisti del movimento considerati uti singuli, parrebbe) c. Facebook[399]. Il Tribunale ha approvato la chiusura dei loro account Facebook con ordinanza ricca di documentazione probatoria[400] e di elencazione di materiali giuridici (nazionali ed internazionali) contrastanti le discriminazioni razziali e i discorsi d'odio[401]. In

[397] V. l'abstract inglese del BverfG/German Federal Constitutional Court's Order of 22 May 2019, 1 BvQ 42/19 nel sito della Corte: <<*The consequences that would arise if the applicant were denied access to its Facebook page but the respondent in the original proceedings were obliged to reopen access clearly outweigh the consequences that would arise if the respondent in the original proceedings were temporarily obliged to restore access but restricting access and disabling the profile were justified. In any event, this applies to the period up to the European elections, for which the applicant has shown particular urgency. The exclusion from using the respondent's services, which, according to the respondent's advertising, are used by more than 30 million people in Germany every month, denies the applicant an essential opportunity to promote its political messages*>>.

[398] "Simile" dice in realtà poco o nulla, dato che i dati fattuali sono decisivi in quiestioni del genere. Qui non esamino il merito, ma solo il profilo del se le piattaforme costituiscano *public forum*: tema su cui ferve il dibattito nella dottrina mondiale (gli scritti in inglese sono già tantissimi, alcuni accennati in questo scritto).

[399] Trib. Roma-sez. dir. della persona e immig. civile, ord. 23.02.2020, RG 64894/2019, XXX c. Facebook Ireland ntd, leggibile in *questionegiustizia.it*. Brevi note in Donato G., *Il potere senza responsabilità dei social media nelle campagne elettorali*, Riv. dir. media, medialaws.eu, 2020/2, che nella decisione sul caso CasaPound ravvisa un approccio para-pubblicistico nel qualificare Facebook, mentre in quella sul caso Forza Nuova un approccio privatistico (p. 362).

[400] La cosa va salutata assai positivamente: è ora che le sentenze riportino direttamente i documenti su cui si basano, invece che rinviare al fascicolo di parte.

[401] Sulla cui portata e raccomandabilità alle piattaforme ci sono però dissensi. Si vedano ad es. le divergenti posizioni tra E. M. Aswad, *To Protect Freedom of Expression, Why Not Steal Victory from the Jaws of Defeat?*, 77 Wash.& Lee L. Rev. 609 (2020), che giudica positivamente la normativa internazionale sull'*offensive speech*, e il saggio (ivi criticato) di Clooney A.-Webb P., *The Right to Insult in International Law*, 48 Colum. Hum. Rts. L. Rev. 1 (2017), più favorevoli al diritto di parola e al *right of insult*, che sarebbero invece non sufficientemente tutelati nella normativa internazionale (di contrario avviso su questo punto il primo a.). Le difficoltà e i travagli di Facebook per gestire problemi (effettivamente complessi) di questo tipo sono esposti in Kadri T.E.-Klonick K., *Facebook v. Sullivan*, cit., parte II (resoconto) e III (suggerimenti) (il saggio in

particolare ha rigettato la domanda cautelare (ex art. 700 c.p.c.) sulla base di due argomenti, autonomi –parrebbe- l'uno dall'altro: le pattuizioni contrattuali tra i ricorrenti e Facebook, da un parte[402], e il dovere di questa di impedire condotte illecite[403], dall'altra. Qui interessa il secondo argomento.

Il dovere di impedimento risulterebbe fondato sull'art. 14 della dir. 2000/31[404] e sull'adesione di Facebook al Codice di Condotta 2016, promosso dalla Commissione UE[405]. Il giudice parrebbe menzionare come fonti del dovere di rimozione anche le fonti interne e sovranazionali da lui elencate (v. pagg. citate dell'ord.): ma non è chiaro quali siano né se siano solo quelle europee sul safe harbour ex dir. 2000/31 ed anche (o invece) le altre citate nella parte iniziale dell'ordinanza. In ogni caso, quest'ultima affermazione è poco precisa, dato che: - nel primo

generale fa un parallelo i problemi per la *old governance* –tribunali tradizionali- e la *new governance* –piattaforme digitali e in particolare Facebook).

[402] Le clausole (*terms of service*) predisposte da Facebook, Twitter e Youtube sono tra loro assai simili e rispecchiano gli insegnamenti impartiti da *Noah v. AOL Time Warner, Inc.*, 261 F. Supp. 2d 532, 536, che le dichiarò valide e vincolanti (E.D. Va. 2003), secondo Mellinger K., *The Section 230 Standoff: Safe Harbor Rollbacks Would Not Solve Alleged "Anti-Conservative Bias" in Social Media Content Moderation*, 10 Wake Forest J.L. & Pol'y 389, a 405-407, per la quale dunque l'abrogazione del § 230 CDA poco cambierebbe, anche perché, in quanto enti privati, non si applica loro il Primo Emendamento).

[403] Tale dovere è menzionato ad es.: alla pag. 8 alla fine di § 1.3; alla p. 14 sub § 1; alla p. 24; alla p. 43 sub § 4Conclusioni.

[404] pp. 7/8 e p. 43. Muto, stante la sua genericità, è allo scopo il cons. 40, pur ricordato dal giudice: "*in certi casi … hanno il dovere di agire*" non dice quali siano questi casi. Poco pertinente è il riferimento a C.G 03.10.2019, *Eva Glawischnig-Piesczek contro Facebook Ireland Limited*, 03.10.2019, C-18/18 (cit. anche in questo articolo).

[405] P. 14 e p. 43. Il Codice di Condotta è leggibile tramite il link presente nella pagina del sito web della Commissione qui indicata, (ove anche il report 04.02.2019 sulla quarta valutazione). V. anche la *Raccomandazione della Commissione sulle misure per contrastare efficacemente i contenuti illegali online* del 01.03.2018. Sulla lotta alla disinformazione v. il *Codice di buone pratiche dell'UE sulla disinformazione* dell'ottobre 2018, promosso dalla Commissione, cui hanno aderito varie Big Tech, e il ponderoso studio condotto per il Paramento Europeo *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States* del febbraio 2019. Questa ed altre iniziative delle piattaforme per fronteggiare il problema dei contenuti "problematici" sono una loro risposta alla sempre più incombente minaccia di regolazione da parte della Commissione UE, secondo Bloch-Wehba H., *Automation in Moderation*, 2020, *Cornell International Law Journal*, Forthcoming, leggibile in https://ssrn.com/abstract=3521619, p. 22 del.pdf)

caso (normativa europea) si tratta di safe harbour e cioè di esenzione, invece che di ascrizione di responsabilità, la quale è lasciata ai diritti nazionali (come si è già osservato in questo scritto); - nel secondo caso (altre norme), non ne risultano che impongano siffatto dovere ad enti che conducano un'attività come Facebook.

Passando al codice di condotta, l'ordinanza romana Forza Nuova c. Facebook lascia intravedere una questione teorica importante, relativa alla vincolatività giuridica degli impegni assunti in quella sede dalle piattaforme. Però non motiva sul punto, mentre invece avrebbe dovuto dimostrare quantomeno che: i) tali impegni di contrasto (e nelle precise modalità discusse in causa) sono presenti nel codice di condotta; ii) il codice stesso è fonte di situazioni giuridiche a favore (o a carico)[406] di Facebook rilevanti per l'ordinamento italiano privatistico. Circa i), va però osservato che le piattaforme si riservarono di esaminare le denuncia alla luce delle loro policies: <<le aziende informatiche la esaminano [la segnalazione] alla luce delle regole e degli orientamenti da esse predisposti per la comunità degli utenti>> e, solo se necessario (intenderei: da esse ritenuto tale), pure alla luce <<delle leggi nazionali di recepimento della decisione quadro 2008/913/GAI, affidando l'esame a squadre specializzate>>. Quindi le piattaforme non riconoscono alcun dovere di agire in base ad un diritto statuale o internazionale, ma solo in base alle loro policies: il che è privo di precettività giuridica, dato che dichiarare di agire secondo le proprie policies nulla aggiunge alle policies stesse. Circa ii), non trattandosi di fonte di diritto generale, l'impegno (anche fosse valido ed efficace) sarebbe fonte di situazioni giuridiche solo pattizie (sovrapponendosi dunque all'altro argomento del giudice): sarebbero forse qualcosa tipo una promessa unilaterale del nostro codice civile, solo che non prevede alcun creditore determinato. Quindi tale ipotetico dovere, da un lato, non può essere ex lege, dato che non ricorreva alcuna fonte ad hoc; dall'altro, nemmeno pattizio, dato che non risulta individuato alcun ordinamento che riconosca vincolatività a simili impegni né alcun creditore investito della correlata situazione giuridica attiva.

[406] A seconda che si guardi il profilo favorevole (diritto di procedere) o quello sfavorevole (dovere di farlo per non incorrere in responsabilità).

Il giudice avrebbe semmai dovuto argomentare sulla base degli artt. 2043-2055 c.c. (magari specificando i profili civilistici di eventuali reati), disposizioni che invece affermano la responsabilità: certamente un soggetto può (ed ha l'onere di) fare quanto in suo potere per evitare di cadere in illeciti civili o penali o comunque di soggiacere ad altri effetti per lui sfavorevoli.

Infine nega il ripristino del profilo personale, e della pagina tematica connessa, Trib. Siena 19.01.2020, n. 2968/2019 RGAC, ord. caut., accogliendo le ragioni di Facebook[407]. Secondo questo giudice, né risulta una violazione contrattuale, "*né la società resistente [Facebook] può seriamente essere paragonata ad un soggetto pubblico nel fornire un servizio, pur di indubbia rilevanza sociale e socialmente diffuso, comunque prettamente privatistico …. Nè ciò può realmente rappresentare una lesione ai diritti fondamentali e inviolabili della persona, garantiti a livello costituzionale, ovvero di autodeterminarsi (art. 2 Cost.), di poter svolgere la propria attività politica in un contesto di uguaglianza e pari opportunità con gli altri esponenti di tutte le altre fazioni (art. 3 Cost.), di ambire (anche in forma professionale e remunerata) a cariche politico istituzionali (art 4, 49 e 51 Cost.), di manifestare liberamente il proprio pensiero (art 21 Cost.). Invero, trattasi di diritti, questi, certamente liberamente esercitabili in contesti diversi, pubblici e, comunque, idonei alla più ampia espressione della propria personalità nell'ambito di una leale competizione politica con la possibilità di condividere con gli appartenenti a quella certa corrente la propria ideologia*". Poi, sul periculum in mora: "*al ricorrente, invero, non è precluso né potrebbe esserlo come conseguenza dell'oscuramento del proprio profilo su Facebook, di adoperare altre piattaforme per la manifestazione, certamente libera ed ampia, del proprio pensiero*". Il giudice senese disconosce l'essenzialità della piattaforma Facebook, ritenendola fungibile con altre modalità di comunicazione: fungibilità, però, che ad oggi non è dato rilevare nel panorama massmediatico.

[407] Leggibile in *Diritto di internet*, con osservazioni di G. Cassano, *Gira la ruota per CasaPound, a Siena prevale il regime privatistico del rapporto, ed il profilo rimane disattivato*, 21.01.2020 (l'a. specifica che il ricorrente era un attivista di CasaPound Siena)

22. Ancora sulla conoscenza richiesta dall'art. 16 c.1

La legge delega aveva diviso in due ipotesi quelle poi riunite dentro lettera a) art. 16 (art. 31 c. lett. f) della legge 39 del 2002). Da questa diversità redazionale, però, non paiono discendere conseguenze, dal momento che è sufficientemente chiaro anche all'interno del d. lgs. 70/2003 che si tratta di due ipotesi.

Si potrebbe pensare ad possibile problema interpretativo intorno al concetto di "appena a conoscenza": cioè intorno al tempo concesso al provider per procedere a rimuovere disabilitare senza uscire dal ombrello protettivo. In realtà va inteso nel senso che, una volta che si provi che era a conoscenza, il tempo a sua disposizione per provvedere è solo quello tecnico per un minimo di riflessione sulla fondatezza dell'istanza e poi procedere alla disabilitazione tecnologica, che a quel punto deve essere immediata[408]. Quindi in pratica oltre i due/tre giorni non si può andare[409] ed anzi si deve stare entro le ventiquattro ore per i contenuti *manifestly unlawful* e immediatamente -e cioè di regola nei sette giorni- per gli altri nella c.d. *Netzwerkdurchsetzungsgesetz* tedesca 01.09.2017[410] (entro

[408] <<*Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-thespot editorial decision whether to risk liability by allowing the continued publication of that information*>>: così la celebre United States Court of Appeals, Fourth Circuit., No. 97-1523, November 12, 1997, *Zeran c. AOL American OnLine*, riportato da Klonick K., *The New Governors*, cit., 1607, ritenuta dall'a. decisione fondamentale per la larga immunità concessa ad AOL e per la sua analisi della *Good Samaritan* provision ex § 230 del *Communications Decency Act* del 1996 – title 47 U.S. Code.

[409] La legge di contrasto al cyberbullismo dà al provider quarantotto ore dal ricevimento dell'istanza per provvedere all'oscurametno (art,. 2 c. 2 L. 29.05.2017 n. 71). Secondo il d.l. 18.02.2015 n. 7 conv. da L. 17.04.2015 n. 43, art. 2 c. 4, in tema di contrasto al terrorismo internazionale, l'autorità giudiziaria può ordinare l'oscuramento e il provider deve provvedere <<immediatamente e comunque non oltre quarantotto ore dal ricevimento della notifica>> (per certi reati; per altri si attende decreto: ivi, c. 3)

[410] Art. 3 § 2 *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG)*, su cui v. T. Wischmeyer, *Making social media an instrument of democracy*, *Eur. law journal*, 2019, 2, 175-176. Questo a. ricorda la sentenza del 1961 della Corte Costituzionale tedesca tra i Länder e Adenauer sulla creazione di una televisione privata, dopo il fallimento delle reciproche trattative, p. 178, e la dottrina tedesca attuale sugli effetti orizzontali dei diritti fondamentali, p. 180. V. pure l'omonima voce in Wikipedia. Secondo un a., la cit. regola tedesca delle 24 ore, posta dalla NetzDG, da un lato,

un'ora, secondo la bozza di regolamento UE 2018 contro la diffusione online di contenuti terroristici[411]). Non rilevano le dimensioni, eventualmente enormi, del provider, che non possono andare a danno dei soggetti lesi dalla sua attività di hosting provider: è suo onere attrezzarsi per provvedere in tal

costituisce illegittima interpretazione della dir., che spetta alla C.G. ex art. 267 TFUE, e, dall'altro, non rispetta la flessibilità della disposizione europea (Claussen V., *Fighting Hate Speech and Fake News. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation*, *Riv. dir. media*, medialaws.eu, 24.10.2018, p. 129). La tesi lascia perplessi, dato che <<*la direttiva vincola lo Stato membro cui è rivolta per quanto riguarda il risultato da raggiungere, salva restando la competenza degli organi nazionali in merito alla forma e ai mezzi*>> (art. 288/3 TFUE). Si tratta dunque non di interpretazione della dir., ma di sua attuazione. E allora si deve passare ad esaminare la compatibilità tra la quantificazione temporale, fissata in sede nazionale (che potrebbe essere troppo stretto per valutazioni minimamente ponderate, come accenna l'a.), e la disposizione elastica europea: a prima vista, però, direi che difficilmente può ravvisarsi incompatibilità (l'interessante tema richiederebbe autonoma trattazione). Il che vale anche a rispondere alla seconda censura mossa dall'a.: la flessibilità, infatti, è insita nel ricorso alla dir. ma non è affatto detto che debba restare nel recepimento nazionale. Se il legislatore europeo avesse voluto imporre inderogabilmente una clausola generale o comunque una norma elastica, avrebbe dovuto ricorrere al regolamento. Per l'a. il termine stretto violerebbe pure il divieto di monitoraggio generale ex art. 15 dir. 2000/31, poiché il termine non può essere rispettato <<without an automatic system monitoring information of all users>> (op. loc. cit., 130): non è chiara però la ragione dell'affermazione, dato che si presuppone la notifica di una diffida specifica. La pensa all'opposto altra dottrina tedesca, per cui i termini nazionali costituiscono addirittura un'interpretazione estensiva: <<*Moreover, the deadlines grant a rather extensive interpretation of the notion of expeditious, that allows the providers to assess the illegality of content in a reasonable and flexible timeframe before action is required. The notion of "expeditious" is also less than clear with national implementations of the E-Commerce Directive refraining from specifying the meaning*>> (Schmitz S.- Berndt C., *The German Act on Improving Law Enforcement on Social Networks (NetzDG): A Blunt Sword?*, December 14, 2018, leggibile in ssrn.com). E' esatta invece l'affermazione di un rischio di incompatibilità con la regola, per cui i rimedi devono essere equi, proporzionati e non eccessivamente costosi ex art. 3 dir. 2004/48 (Claussen V., *Fighting Hate Speech and Fake News*, op. loc. cit.; l'a. scrive di art. 3 E-Commerce Directive, invece che dir. 2004/48, ma dovrebbe essere una svista): ma anche qui servirebbe trattazione apposita, anche se parrebbe trattarsi di termine ragionevole, dato che sono le stesse Big Tech ad averlo accettato nel *Codice di condotta per lottare contro le forme illegali di incitamento all'odio online* del 2016, sopra cit. (se pur con alcune limitazioni).

[411] proposta di regolamento UE relativo alla prevenzione della diffusione di contenuti terroristici online 12.09. 2018, COM 2018) 640 final-2018/0331 (COD), art. 4 § 2.

senso con personale dedicato[412]. In alternativa alla soluzione unica, si potrebbe forse distinguere il modello di business, da cui segue un diverso tipo di content moderation strategies, essendone ad es. state individuate tre: *Artisanal* (operanti su piccola scala, come Vimeo ed altri), *Community-reliant* (largamente basati su collaborazione volontaria, come Wikimedia e Reddit) e *Industrial* (come Facebook e Google)[413].

[412] La legge australiana del 2019, emanata dopo il massacro di Christchurch, sanziona penalmente chi non rimuove "expeditiusoly" certi materiali: <<*the Act makes it an offence for social media companies to fail to "ensure the expeditious removal" of abhorrent violent material on their service, or for hosting services to fail to "expeditiously cease hosting" such material*>>, mentre concede un "*reasonable time*" per la denuncia alla *Australian Federal Police* (Douek E., *Australia's 'Abhorrent Violent Material' Law: Shouting 'Nerd Harder' and Drowning Out Speech*, 94 Australian Law Journal 41 (2020), leggibile in https://ssrn.com/abstract=3443220), p. 3-4 del.pdf). A quanto tempo corrisponde *Expeditiously*? <<*It is likely therefore that timeframes will be measured in hours and minutes, rather than days*>> (Douek E., *Australia's 'Abhorrent Violent Material' Law:*, cit., p. 6 del.pdf). Secondo Campobasso M., *L'imputazione di conoscenza nelle società*, Giuffrè, 2002, la società non è responsabile oggettivamente per tutti i dati che riceve (p. 346 ss), ma solo di quelli che sarebbero stati da lei utilizzabili, se avesse adottato procedure di corretto trattamento o meglio di efficiente organizzazione allo scopo (p. 359 ss e spt. § 5.10 alle p. 363 ss): <<*la negligenza nella gestione delle informazioni può essere così valutata in sede di applicazione delle norme fondate sulla conoscenza come elemento che preclude alla società l'accesso al regime favorevole previsto per l'ignoranza o la buona fede, quando il rispetto di normali procedure di corretto trattamento avrebbe consentito di fare uso nella vicenda specifica del dato già in suo possesso*>> (p. 364) e "*Come corollario processuale... si può ritenere che la prova della conoscenza di una società è raggiunta in primo luogo con la dimostrazione che l'inforamzione rilevante era nota ad uno dei soggetti che possono direttament imputare il proprio sapere all'organizzazione in base ai principi della disciplina della rappresentanaza …. Ove però non sia possibile dimostrare tali circostanze, è altresì sufficiente allegare che il dato era posseduto dall'organizzazione in condizioni, che facciano presumere la possibilità di utilizzarlo. Sarà poi onere della società rovesciare questa presunzione, dimostrando di non aver potuto attingere all'informazione nella vicenda controversa per ragioni non imputabili a cattiva gestione*" (p. 366, nota 80). Il principio è applicabile al caso nostro.

[413] Caplan R., *Content or context moderation?*, cit., p. 16 ss. Altre tassonomie in Grimmelmann J., *The virtues of moderation, Yale journal of law and technology*, vol. 17/2, 2015, sub II, p. 55 ss (saggio approfondito e citato da molti aa. successivi): quanto alle tecniche di moderazione, l'a. prospetta i) esclusione, ii) prezzamento (pricing), iii) scelte organizzative sui flussi tra mittenti e destinatari, iv) norm setting. Quanto alla modalità per attuare tali condotte, egli distingue tra i) automatica/manuale, ii) trasparente/segreta, iii) ex ante/ex post, iv) centralizzata/distribuita.

In pratica, per le grandi piattaforme (tipicamente Youtube[414]), nonostante richieste ingenti o massive di rimozione/disabilitazione come possono fare i colossi mondiali dell'entertainment, il problema non si porrà: infatti le grandi piattaforme procederanno in via automatica, magari dopo aver ricevuto le richieste in formati standardizzati predisposti ad hoc[415], se non addirittura via estesa a tutto il flusso transitante su di esse[416] (il che però può dirsi costituire censura preventiva/prior restraint per l'utente uploader[417]).

Più significativo invece è il problema della interpretazione del concetto di <<effettivamente a conoscenza>> e di <<essere al corrente di>>, presenti nella prima delle due sotto ipotesi della lettera a) e, rispettivamente, nella lettera b). Il problema attiene al dettaglio di informazione che il titolare del diritto violato deve comunicare al provider: in particolare il punto circa la necessità o meno di comunicare anche la URL del file contenente il

[414] Tutti coloro che si occupano di politica economica, applicata al copyright, sanno che l'art. 17 della dir. UE 2019/790 è stato voluto specificamente per costringere Youtube a pagare royalties sui contenuti messi on line (così Bridy A., *The Price of Closing the "Value Gap"*, cit., 325). La tesi dell'industria musicale statunitense, infatti, è che il safe harbour del DMCA, da un lato, è una delle principali cause delle violazioni di copyright e, dall'altro, stanti gli incentivi economici che produce, conferisce notevole potere agli ISP nella negoziazione di licenze: così Etcovitch D., *DMCA S. 512 Pain Points: Music and Technology Industry Perspectives in Juxtaposition*, in *Harv. jour. of law & tech*., 2017, vol. 30/2, 550-551 (nelle pagg. seguenti l'a. ricorda che, secondo l'opposta narrativa delle Big Tech, invece, il safe harbour è utile per promuovere i contenuti e i servizi internet). Per vero questa ragione è stata alla base dell'introduzione del DMCA: v. Matteson J.D., *Unfair Misuse: How Section 512 of the DMCA Allows Abuse of the Copyright Fair Use Doctrine*, cit., 5-6.

[415] L'ultima decisione nella lite *Viacom v. Youtube* (del 2013), cit. a nota 183, ricorda che Viacom nel 2007 aveva avvisato della violazione da parte di 100.000,00 video, che Youtube rimosse entro il seguente giorno lavorativo (p. 6).

[416] Gorwa R.-Bins R.-Katzenbach C., *Algorithmic content moderation: Technical and political challenges*, cit., p.9. Secondo gli aa. (pp. 4-5), la distinzione essenziale da fare per la algorithmic moderation è tra il *matching* (confronto con quanto già presetne nei database tramite la tecnica c.d *hash matching* -anche nella forma del *perception hashing*, che permette delle variazioni che altrimenti, pur se minime, farebbero ottenere il via libera-, per vedere se l'hash, cioè l'impronta informatica, di un documento già presente si ripete in quello sotto esame), da una parte, e la *classification/prediction* (opera di categorizzazione: spam, hate speech etc., se non c'è un termine di confronto nel database), dall'altra.

[417] Llansó E.J., *No amount of "AI" in content moderation will solve filtering's prior-restraint problem, Big Data & Society*, 2020, 2 ss

materiale illecito. Non si sottovaluti la questione, come si potrebbe fare ritenendo che in fondo non è così oneroso per il titolare comunicare la URL del file da lui individuato. Infatti non è così oneroso, se si tratta di uno o pochi file. Quando però si tratta di violazioni massive, potrebbe essere alquanto o molto fastidioso: anche perché – in mancanza di bottoni automatici di segnalazione nel browser (tipo quelli di "aggiungi ai preferiti") e cioè se si deve fare un copia/incolla della url- basta sbagliare un carattere per non poter più accedere al file medesimo (per non dire poi della tecnica talora utilizzata di caricare i file illeciti su server via via diversi, i cui nomi o numeri IP cambiano in continuazione, c.d. siti alias).

Dalla normativa europea sembra abbastanza chiaro che non sia richiesta l'indicazione della URL[418]. Il riferimento alla conoscenza ("essere al corrente" dell'illiceità o di fatti sintomatici in tale senso), presente nella dir., induce a ritenere sufficiente che il provider abbia quei dati che gli bastano per individuare rapidamente lui stesso il file illecito: sì che, nel caso ad esempio di riproduzioni o comunicazioni di opere dell'ingegno audiovisive, basterà il titolo dell'opera. Anzi man mano che sarà chiaro cosa permettono i filtri oggi disponibili sul mercato, la cui adozione costituisce comportamento diligente e la cui mancata adozione costituisce comportamento negligente[419], si potrà precisare meglio quali sono le informazioni sufficienti, affinché il provider le inserisca in questi filtri; filtri che non servono solo per prevenire futuri caricamenti ma anche per individuare i file tra quelli già caricati[420].

Il problema potrebbe essere processuale, nel senso che il soggetto leso o –soprattutto- il CTU possono non conoscere

[418] Ci si può chiedere se basti allora la singola comunicazione da parte del *quisque de populo*, magari tramite un semplice *flag*: per Brown N.I., *Deepfakes and the weaponization of disinformation*, cit., 51, la risposta è negativa, dato che il flag immotivato permette alle piattaforme di *bury their heads in the sand.*

[419] Salvo un problema di rapporto tra costi e dimensioni del provider, certo giuridicamente rilevante e che meriterebbe specifico esame.

[420] Gli utilizzi dei filtri si concentrano in due aree: violazioni di diritto d'autore e propaganda terroristica (Heldt A.P., *Upload-Filters: Bypassing Classical Concepts of Censorship?*, Jipitec, 2019, p. 61, § 15: l'a. riferisce di altro articolo secondo cui che il 99.5% delle deunce viene trattato tramite l'abbinamento automatico operato dal software Content-ID).

esattamene i software (l'algoritmo) di gestione dei file, adoperato dalla piattaforma. La sufficienza dell'informazione fornita potrebbe venir giudicata in relazione a quest'ultima, ma la segretezza del software (gelosamente custodita) non permette di dire cosa la piattaforma può realmente fare: per cui potrà ad es. indurre a ritenere insufficiente una comunicazione, che invece in quel contesto aziendale era più che sufficiente per una velocissima individuazione e rimozione/disabilitazione.

Si potrebbe allora teoricamente distinguere tra casi, in cui il soggetto leso notificasse moltissime violazioni, da quello in cui ne notificasse una sola o poche (quante però?): per poi concludere che solo nel secondo caso fosse tenuto ad indicare la URL (favor per il soggetto leso, ad es. per evitargli il rischio di errori nella comunicazione). Si potrebbe però opporre che è proprio nel primo caso che il provider deve aver più precisa informazione: proprio perché la comunicazione concerne violazioni massive, senza le URL egli dovrebbe impiegare tempo e risorse significative (favor per il provider). Quest'ultimo, però, anche senza scomodare le responsabilità aquiliane oggettive, nella composizione degli interessi confliggenti, è un'onere che dovrebbe gravare sul provider, costituendo rischio tipico di impresa da lui governabile (ad es. predisponendo formulari online, che il soggetto leso ha l'onere di compilare, i cui dati egli possa trattare in automatico).

Anzi, visto che, dopo il ricevimento della comunicazione, la responsabilità diventa contrattuale (ex lege), si tratterà di determinazione della prestazione dovuta: la quale, alla fine e per la stessa ora esposta ragione, dovrà comprendere anche il farsi carico dell'individuazione e rimozione/disabilitazione dei -per quanto numerosi- file illeciti denunciati. La quantità dei file potrà avere rilevanza nella determinazione del profilo temporale, per provvedere in tale senso: quanto più numerosi, tanto maggiore sarà il tempo di cui potrà fruire[421]. Ma, seppur con

[421] La diligenza in base agli standard tecnici settoriali (qualità dei filtri disponibili; questione non facile, dato che ce ne saranno di diversi livelli di costo) dirà quanto tempo serve ad un operatore per eseguire tali operazioni: dovrà indicare quale è il minomo necessario, non essendoci ragione per impiegarne di più (non sarebbe un provider diligente). A causa dell'automazione quasi totale, Google ad es. ha ricevuto intimazioni di rimozione di 558 milioni di pagine web nel 2015 e ha esaminato 75 milioni di intimazioni al mese nel 2017 (Gray J.E., *Google Rules*, cit., 118: nella pagg. ss. v. esame del filtraggio eseguito di propria iniziativa). Secondo altri, Google tratta ogni giorno due milioni di tali intimazioni

qualche dubbio, direi che non si possa onerare il soggetto leso di individuare e comunicare l'esatta URL di ogni file illecito: è sufficiente che il provider possa con facilità individuarlo[422]. Ciò naturalmente a meno che meno che vigano norme in senso contrario, che però nel diritto UE e nazionale mancano. Lo stesso § 512.c.3.A del 17 US Code, pur assai più dettagliato, si limita ad onerare il soggetto leso di inserire nella comunicazione la <<*(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site. (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material*..>>[423]. Il criterio di ragionevolezza nelle indicazioni per localizzare il file è utilizzabile pure da noi: discende dalla regola di buona fede o correttezza (nella fase precontrattuale o di esecuzione di contratto, a seconda di come si qualifichi la fattispecie) oppure da quella di non colpa (se si opti per la qualificazione aquiliana come concorso creditorio ex artt. 1226-2056 cc).

E se la Direttiva non richiede la indicazione della URL, c'è da pensare che un eventuale richiesta in tal senso della normativa nazionale sarebbe in contrasto con la stessa. Il fatto, però, è che nemmeno nella normativa nazionale vi sono elementi per pensare che sia necessario indicare la url. La Corte di Cassazione ha affrontato la questione nell'altra causa parallela, sempre nella vertenza *RTI c. Yahoo*, con la sentenza 19 marzo 2019 n. 7708 (§ 5.8). Ha concluso in una direzione simile a quanto indicato e cioè che sono i profili tecnico-informatici decisivi per stabilire, se la mera indicazione del nome della trasmissione è sufficiente oppure se serva la url del file (e ciò all'epoca dei fatti sub iudice,

e nel 2016 ha rimosso 900 milioni di link a file presuntivamente illeciti (Penney J., *Privacy and Legal Automation: The DMCA as a Case Study*, cit., 426, per cui il DMCA può essere descritto come *predominantly "algorithmic copyright enforcement"*, ivi).

[422] Tosi E., *La disciplina applicabile all'hosting provider*, cit., 269.

[423] La disposizione è stata però criticata per la sua ambiguità dall'indagine svolta dall'US Copyright Office: v. il *Section 512 of title 17. A report of the Register of Copyright, May 2020*, che suggerisce di considerare l'ipotesi di precisarla (p. 4).

potendo la tecnica mutare). Secondo la S. C. si tratta di un profilo di merito che presuppone un ineludibile accertamento in fatto. Quest'ultimo punto, però, è di dubbia esattezza, poiché il giudizio di fatto riguarda la disponibilità di questo o quel dispositivo tecnico sul mercato e a quali condizioni; costituisce invece giudizio di diritto -precisamente di applicazione del canone diligenza/negligenza- accertare se il provider era tenuto meno ad adottarlo e quindi se aveva o meno l'onere di indicarlo al soggetto leso[424]. Quanto alla necessità di indicare l'url da parte del soggetto leso (ma in verità da parte di chiunque), la giurisprudenza è divisa e diversi autori l'affermano[425].

Non costituisce argomento in senso contrario, alla non necessità di indicazione dell'url, il divieto di doveri di monitoraggio generale, come taluno ha addotto[426]. Riguardo alle violazioni di copyright, ad es., l'indicazione di alcuni dati, come il nome dell'opera violata e del soggetto che risulta uploader (o del sito che ospita), dovrebbe impedire che la successiva condotta del provider rientrasse nel concetto di cui all'art. 16 d. lgs. 70/2003[427].

23. Una ricostruzione della disciplina posta dall' art 16 c.1

Un a. ha proposto un articolata interpretazione del c. 1 dell'art. 16[428], che, se ben comprendo, dovrebbe essere così riassumibile. La disciplina è divisa in due fattispecie principali: la prima costituita dalla lettera a) (prima parte: "… a condizione

[424] La Suprema Corte ha censurato la sentenza di appello per non aver eseguito questo accertamento (sub § 5.8).

[425] Wang J, *Regulating hosting ISP's responsabilities for coyright infringement*,. cit., 165

[426] L'industria musicale, precisamente (Etcovitch D., *DMCA S. 512 Pain Points,* cit., 555).

[427] Contrario Etcovitch D., *DMCA S. 512 Pain Points*, op. loc. ult. cit., perchè il DMCA al provider non chiede altro che rispondere alla *notice*. Però nulla dice sull'attività preliminare per dare la giusta risposta, né obbliga ad accogliere la richiesta: si limita a dire che la rimozione/disabilitazione a certe condizioni lo esenta da responsabilità. Si v. poi la *representative list* che il DMCA permette al titolare di inviare al provider in caso di violazioni multiple (<<*Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site*>>: § 512.c.3.A.ii): disposizione che pare confermare la non necessità di precisi url per ogni violazione. Il punto è però controverso: Etcovitch D., *DMCA S. 512 Pain Points,* op. loc. ult. ci 556-557

[428] Piraino, cit., 500-502.

che detto prestatore: a) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita (…)") e dalla lett. b) dell'articolo 16; la seconda fattispecie, invece, costituita dall'articolo 16 lett. a) seconda parte, relativa al risarcimento ("a condizione che detto prestatore: a) (…) per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione"). Nel primo caso si disciplinano i rimedi non risarcitori, nel secondo quello risarcitorio. Quanto alla prima fattispecie, la condizione di conoscenza comunque acquisita (si badi: in qualunque modo acquisita) impone all'hosting provider di adottare le regole di perizia professionale e cioè adottare le misure necessarie alla cooperazione per verificare il contrasto degli illeciti commessi, come proverebbero pure il cons. 46 (sul dovere di immediata rimozione/disabilitazione appena il provider abbia consapevolezza dell'illiceità) e il cons. 48 (sulla pretendibilità di una condotta diligenza del provider) della dir. Ed allora afferma questo a.: i) se si tratta di conoscenza semplice –cioè "contezza della possibile natura illecita della comunicazione o dell'utilizzo delle informazioni memorizzate"-, l'obbligo di cooperazione si concretizza nel dovere di segnalare all'autorità giudiziaria o amministrativa l'ipotesi di illecito e offrire gli elementi utili per risalire all'identità dell'autore della violazione; ii) se invece c'è un positivo accertamento giudiziale o amministrativo, sorge per l'intermediario l'obbligo di provvedere subito a rimuovere o disabilitare: se non provvede così, è responsabile dei danni prodotti dalla protrazione della violazione per concorso di cause ex articolo 1227 comma 1 ed in via solidale ex. art. 2055. Quanto alla seconda fattispecie (rimedio risarcitorio), questa ricorre quando l'illiceità è manifesta (anziché solo presunta): anche in tale caso il provider deve adottare regole di perizia professionale, che però non si limiteranno al dovere di segnalare e cooperare: imporranno piuttosto la rimozione dei contenuti e la disabilitazione dell'accesso, altrimenti dovendosi ravvisare alla responsabilità in concorso con l'autore della violazione in misura che potrebbe essere anche paritaria. Solo così si recupera la conformità alla dir.

Sull'articolata proposta sono possibili alcune osservazioni:

i) la conoscenza dell'illiceità della prima parte dell'art. 16 c. 1 lett. a) non è meno sicura di quella della sua seconda parte,

anzi forse lo è di più: "effettivamente a conoscenza del fatto che l'attività è illecita" vs. "fatti che rendano manifesta l'illiceità". Cambia invece l'oggetto della conoscenza: la prima è la conoscenza effettiva e diretta della illiceità dei file, la seconda solo induttiva (indiretta), in quanto basata su fatti che dovrebbero indurre con facilità alla stessa convinzione. Come detto sopra, la logica appare chiara: il provider perde il safe harbour se sa effettivamente della illiceità o se avrebbe dovuto saperlo in base a fatti assai probanti. Questo secondo livello di consapevolezza è abbassato rispetto al primo, forse perché per le azioni risarcitorie sono meno invasive di altre (penali, misure detentiva; o amministrative, sospensioni o chiusura di attività, etc.), per cui la composizione del conflitto di interessi si sposta a favore del soggetto leso. E' dunque antiletterale sostenere che la conoscenza della prima parte della lett.a) sia meno certa di quella della seconda parte, essendo una "contezza della possibile natura illecita della comunicazione"[429] ovvero "mera conoscenza di una presunta attività illecita"[430]: il dettato ("a condizione che non sia effettivamente a conoscenza"), invece, si riferisce ad una conoscenza effettiva e dunque dice l'opposto;

ii) affermare che solo nel caso del risarcimento del danno (fatti denotanti una illiceità manifesta) sia doverosa la rimozione/disabilitazione anche senza ordine dell'autorità, contrasta col dato testuale: la lett. b) infatti, fonte di tale dovere, comunque la si interpreti, è riferita ad entrambi i casi della lett. a). Quindi il giudice non può disapplicarla in uno dei due casi ed applicarla solo all'altro;

iii) inoltre è da vedere se la difformità dalla dir. (laddove si pretende l'ordine dell'autorità per la rimozione/disabilitazione: difformità innegabile), una voltata tentata inutilmente l'interpretazione ad essa conforme, si possa risolvere con disapplicazione –come se si trattasse di contrasto con norma UE direttamente applicabile- oppure se debba passare (come parrebbe) per la dichiarazione di incostituzionalità della legge delega o del decreto delegato;

iv.i) non si può limitare l'obbligo di segnalazione al caso di conoscenza minore ex lett. a), prima parte. Intanto è posto dall'art. 17, e non dall'art. 16, e l'art. 17 si applica a tutti i tipi di

[429] ivi, p. 500.

[430] ivi, p. 501.

provider e in qualunque circostanza si vengano a trovare. iv.2) se poi lo si ricava non dall'art. 17 ma dalla diligenza/perizia professionale (cons. 48 dir.), pure questa opera non solo quando i fatti manifestamente facciano propendere per l'illiceità, ma anche quando il provider abbia comunque effettiva conoscenza dell'illiceità stessa (art. 16.1 lett. a, prima parte): e cioè pure per il caso di conoscenza semplice. In altre parole, la presunta diligenza/perizia professionale, circa il dovere di segnalazione, non permette di distinguere tra i due tipi di conoscenza emergenti dalla lett. a);

v) è assai dubbio che sia la diligenza professionale a portare all'obbligo di segnalazione all'autorità. Essa porterà semmai ad adottare congrui filtri, non alla denuncia alla autorità: quest'ultima costituisce un dovere civico, che può diventare giuridico solo se una norma espressamente lo preveda (art. 23 Cost.). Non pare avere molto a che fare con la diligenza professionale, la quale riguarda o la modalità esecutiva della prestazione (responsabilità contrattuale) o la cautela nelle proprie azioni per non procurare danni a terzi (responsabilità aquiliana).

vi) non è chiaro (almeno a me) poi il riferimento al concorso di cause ex art. 1227 c. 1, qualora non provveda tempestivamente alla rimozione/disabilitazione. Questa norma regola il concorso di condotta tra danneggiante e danneggiato, mentre qui si parla di concorso tra utente uploader e provider nella causazione del danno al soggetto leso: di quest'ultimo nel passaggio in esame non si menziona alcuna condotta concorsuale, che sarebbe invero difficilmente immaginabile.

vii) riferire il cons. 46 solo alla prima parte della lett. a) (rimedi non risarcitori), per sostenere il dovere di cooperazione con segnalazione all'autorità, come pare fare la dottrina in esame, non parrebbe giustificato per due motivi: da un lato, il cons. parla di rimozione/disabilitazione e non di cooperazione/segnalazione; dall'altro, si limita ad anticipare l'art. 16 lett.b) e dunque si applica a qualunque caso, in cui abbia notizia della illiceità, senza distinzioni qualitative all'interno di tale concetto (in particolare, senza possibilità di distinguere tra le due sottofattispecie presenti nell'art. 16 lett. a).

24. L'art. 16 c. 2

Secondo il comma 2, uguale nei due testi (nazionale ed

europeo), non si applica l'esenzione se l'utente agisce sotto l'autorità o il controllo del provider. Il che non è sorprendente e non serviva norma che lo precisasse: tutto il meccanismo del safe harbour per il provider si basa sulla sua neutralità rispetto ai contenuti, per cui è ovvio che sia fruibile quando l'utente (l'uploader del materiale illecito) addirittura agisca sotto l'autorità o il controllo del prestatore. Non solo in tali casi non è dato safe harbour, ma molto probabilmente opererà la responsabilità dei padroni e committenti ex artt. 2049 cc[431]: la quale, come noto, comporta responsabilità solidale ex art. 2055 di entrambi i titolari del rapporto collaborativo[432].

Andrebbe piuttosto approfondito il concetto di "autorità" e di "controllo". Il primo sembra ricorrere nei contratti tipo quello di lavoro subordinato, mentre escluderei il contratto di lavoro autonomo come l'appalto, tranne che l'appaltatore sia nudus minister. Il concetto di "controllo" è più nebuloso e quindi potenzialmente più ampio: c'è però una relazione stretta e quasi biunivoca tra i due concetti. Infatti se si ha autorità su una persona, si ha pure possibilità di controllarla: in mancanza, l'autorità sarebbe solo declamata ma inesistente nei fatti. Reciprocamente, chi controlla una persona (nel senso di potere influire unilateralmente sulle sue scelte, almeno in parte qua) può ben dirsi abbia autorità sulla stessa.

L'applicazione può presentare difficoltà. Ci si può ad es. domandare se ricorra il controllo del provider, quando questi si riservi la facoltà contrattuale verso l'utente di controllare e rimuovere il materiale caricato e di farlo a sua discrezione o magari –in maniera più ristretta- ogni volta che giunga un reclamo da parte di terzi[433]. Ed in effetti qualche decisione lascia intravedere un ragionamento di questo tipo. La risposta non è facile: alla fine, però, come sopra accennato circa l'analoga

[431] V. Comporti M., *Fatti illeciti: le responsabilità oggettive. Artt. 2049-2053,* in Il *cod. civ. Comm.* dir. da Busnelli, Milano, 2009, 100 ss. che discute l'applicabilità della disposizione ai principali contratti collaborativo, oltre a quello di lavoro dipendente. Lo esclude T. Pasquino, *Servizi telematici e criteri di responsabilità*, cit., 272, che esclude pure la responsabilità da attività pericolosa ex art. 2050 (v. analiticamente ivi, p. 273 ss.)

[432] Comporti M., *Fatti illeciti: le responsabilità oggettive. Artt. 2049-2053,* cit., 86; Franzoni M., *Dei fatti illeciti. Art. 2043-2059,* cit., sub art. 2049, p. 356.

[433] Inevitabilmente clausole di questo tipo, anzi con maggiori trasferimenti di diritti, sono fatte accettare dalle piattaforme ai loro utenti.

prescrizione contenuta nel cons. 42, il concetto di controllo pare alludere ad un controllo regolarmente esercitato nei fatti e non semplicemente riservato in via pattizia. In altre parole il controllo deve essere in atto, non solo in potenza..

Si pensi al caso della fotografa statunitense, che ha spiacevolmente scoperto –in sede giudiziale- che un sito giornalistico aveva divulgato una fotografia presente nel suo account Instragram e che lo aveva fatto lecitamente (dopo aver invano tentato di essere autorizzato in via negoziale). ciò perché gli utenti di Instagram da un lato trasferiscono a questo i diritti sui materiali caricati e dall'altro l'autorizzano a darli in licenza a terzi, solo che usino la sua API-Application Programming Interface[434]. Ebbene, questo non integra il requisito dell'autorità né del controllo da parte di Instagram: per cui, se il materiale caricato dalla fotografa fosse stato illecito, Instagram non avrebbe perso il diritto al safe harbour.

Per quanto tutti i grandi provider si riservino a questa facoltà, probabilmente poi nei fatti non controllano alcunché: a meno che ciò venga in via automatica tramite i filtri oppure dopo denuncia di illecito. Ma il concetto di controllo qui richiamato non è quello operabile tramite i filtri, bensì quello realmente praticato (e, probabilmente, da un umano, non da software), da un lato, e con vincolatività giuridica dall'altro. Autorità e/o controllo ricorrono ad es. nel caso di articoli giornalistici di un giornale cartaceo, che venga riprodotto on line dalla società editrice[435]: si tratta infatti di responsabilità editoriale, nel qual caso appunto l'editore non può certo invocare il safe harbour (anche se mancasse normativa ad hoc). In altre parole bisogna che l'autorità o il controllo venga normalmente esercitato ed in toto, non solo circa le policy aziendali della piattaforma, in modo che la condotta possa dirsi riconducibile alla piattaforma,

[434] V. mio post sulla sentenza statunitense Southern District Court Of New York, *Sinclair v. Ziff Davis-Mashable*, 13.04.2020, in albertinilawfirm.eu.

[435] Così C.G. 11.09.2014, C-291/13, *Sotiris Papasavas*, §§ 37-46, che però inspiegabilmente nega il safe harbour all'editore richiamando solo il cons. 42 e non –come sarebbe stato più esatto- l'art. 14 § 2, dir. 2000/31, pur menzionando la presenza di controllo sull'informazione (§ 45). Il ragionamento allora è poco limpido, parendo confondere la presenza/assenza di controllo ex art. 14 § 2 dir. 2000/31 con la passività/attività ex cons. 42: che potrebbero anche forse sovrapporsi, ma andrebbe spiegato (analogamente, poca limpidezza in Riordan J., *The liability of internet intermediaries*, cit., 404-405).

anziché all'utente.

Si veda quanto osserva il giudice Stanton nell'ultimo provvedimento giudiziale (del 2013) nella lite *Viacom c. Google-Youtube*: <<*The only evidence that YouTube may have steered viewers toward infringing videos is as follows: YouTube employees regularly selected clips to feature "with conspicuous positioning on its homepage" (RSUF 331), and on two occasions chose to highlight a clip-in-suit. YouTube asserts, without contradiction, that the creators of the work contained ln the first clip-in-suit, "the premiere of Amp' d Mobile's Internet show 'Lil' Bush,'" made the clip available on YouTube, and thatYouTube featured the second clip-in-suit, "a promotional video from comedy group Human Giant entitled "Illuminators!,"' on its homepage at the request of Human Giant's agent (id. 332). No reasonable jury could conclude from that evidence that YouTube participated in its users' infringing activity by exercising its editorial control over the site.Thus, during the period relevant to this litigation, the record establishes that YouTube influenced its users by exercising its right not to monitor its service for infringements, by enforcing basic rules regarding content (such as limitations on violent, sexual or hate material), by facilitating access to all user-stored material regardless (and without actual or construct knowledge) of it was infringing, and by monitoring its site for some infinging material and assist some content owners in their efforts to do the same. There is no evidence that YouTube induced its users to submit infringing videos, provided users with detailed instructions about what content to upload or edited their content, prescreened submissions for quality, steered users to infringing videos, or otherwise interacted with infringing users to a point where it might be said to participated in their infringing activity*>>[436].

Un recente provvedimento d'appello statunitense ha esaminato se il newsfeed di Facebook lo costituisca content provider ex art. § 230(f)(3) CDA, tale essendo la <<*entity that is responsible, in whole or in part, for the creation or development of information provided*>>. In tale caso infatti non si applicherebbe il safe harbour del Buon Samaritano di cui alla

[436] US District Court-Southern Court of N.Y., *Viacom ed altri c. Youtube-Google*, 18 aprile 2013, caso 07 civ. 22103-LLS, p. 19-20, già ricodata sopra.

precedente lettera (c)(1)[437]. Secondo la Corte, Facebook non può essere ritenuto content provider e in particolare non è il developer della informazione (come invece l'allegazione attorea[438]): *<<the term "development" in Section 230(f)(3) is undefined. However, consistent with broadly construing "publisher" under Section230(c)(1), we have recognized that a defendant will not be considered to have developed third-party*

[437] US Court of Appeals, Secondo Circuito, *Stuart Force e altri c. Facebook*, docket n° n° 18-397, 31 luglio 2019, reperibile nel relativo database. Si trattava di una richiesta di danni per aver Facebook contribuito alle comuncazioni tra aderenti ad Hamas circa attentati avvenuti in Israele tra il 2014 e il 2016 a carico di cittdini statunitensi. Secondo la Corte, per far operare il Good Samaritan safe harbour ex § 230(3)(1) CDA, bisogna superare i due punti di dissidio tra le parti: cioè capire se l'allegazione attorea era nel senso i) che Facebook aveva agito come publisher della informazione dannosa, e ii) nel senso che quest'ultima proveniva da Hamas o Facebook (p. 29). Circa i), il presupposto è che il safe harbour operi solo se l'azione proposta consideri il convneuto come publisher, altrimenti non operando, e potendo egli semmai essere ritenuto responsabile. La corte quindi nela prima parte della Discussion (sub II.A) discutendo il primo punto, afferma che secondo l'allegazione svolta, Facebook è un publisher e rigetta la difesa degli attori, secondo cui invece il ruolo di Facebook non era quello di editore ma solo di "contributore" tramite i suoi algoritmi (p. 21-22; quindi un caso di *secondary liability*, suppongo). La questione è sottile (v. il seguente § 230 (e) (3) CDA, per cui <*No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section*>), ma da noi non si pone, visto che l'articolato europeo e nazionale esclude in toto ogni responsabilità e non solo quella editoriale. Nella seconda parte della discussion la corte esamina l'altro aspetto (sub ii). v. sub II.A, p. 41 ss) con le considerazioni brevemente ricordate nel testo, per concludere che Facebook non è un content provider. C'è però una vigorosa opinione dissenziante del giudice Katzmann, per il quale non è publisher chi si limita a mettere in contatto le persone: <<*when a plaintiff brings a claim that is based not on the content of the information shown but rather on the connections Facebook's algorithms make between individuals, the CDA does not and should not bar relief*>>, p. 3. Ritiene invece che le piattaforme (o meglio i loro soggetti apicali, stante il principio *societas delinquere non potest*) possano incappare in responsabilità penale per correità (*complicit in incitement to genocide*) Hakim N., *How Social Media Companies Could Be Complicit in Incitement to Genocide*, in *Chicago Journal of International Law*, Vol. 21/1, sub IV e V, p. 103 ss (l'a. non menziona il § 230 CDA). ; Yue N., *The "Weaponization" of Facebook in Myanmar: A Case for Corporate Criminal Liability*, in *Hastings law journal*, vol. 71, 2020, p. 813 ss sub V, per cui il diritto penale internazionale potrebbe anche ravvisare responsabilità penale di Facebook nel dramma dei Rohingya in Myhanmar (e poi v. p. 831-832: <<*Facebook's decisions impact who gets a voice and who doesn't, which significantly impacts the spread of speech. By curating content on its platform, Facebook acts less like a non-engaging bystander and more like an active participant in the promulgation of inciteful speech.*>>)

[438] P. 41-42 della sentenza.

content unless the defendant directly and "materially" contributed to what made the content itself "unlawful.". (…) This "material contribution" test, as the Ninth Circuit has described it, "draw[s] the line at the 'crucial distinction between, on the one hand, taking actions... to... display ... actionable content and, on the other hand, responsibility for what makes the displayed content [itself] illegal or actionable.'">>[439]. Infatti gli algoritmi di Facebook sono "content neutral", dato che si limitano al matching tra utenti, prescindendo dai contenuti, i quali rimangono inalterati[440]. Né l'esito cambia per il fatto che rendono l'informazione più *visible, available and usable*, costituendo ciò normale attività editoriale[441] (che, come si è detto in nota, è il presupposto per applicare il safe harbour statunitense).

Analogamente in *Daniel c. Armslist* era stato chiesto di condannare Armslist.com, un sito bacheca per la compravendita di armi, perché il suo website era stato costruito per eludere la normativa vigente in materia e dunque doveva essere ritenuto corresponsabile dell'omicidio plurimo compiuto tramite armi così acquistate (presso un terzo venditore privato). La Corte Suprema del Wisconsin, però, pur dando atto che il safe harbour è opponibile solo a chi fa valere una responsabilità editoriale, interpretò la domanda giudiziale non come responsabilità da negligenza/violazione del duty of care, bensì appunto come responsabilità da "publisher o speaker" di informazioni di terzi[442] e concesse dunque ad Armslist.com il safe harbour[443]. Per la Corte, il sito costituiva infatti un neutral tool, suscettibile pure di usi leciti, per cui il suo titolare non può dirsi creator o developer dell'informazione illecita e dannosa (annuncio di vendita armi), per cui era causa[444]. La sentenza è poi interessante perché chiarisce in modo deciso che il § 230 CDA, non

[439] p. 42 della sentenza.

[440] p. 47/8 sdella sentenza.

[441] p. 49 della sentenza. Nemmeno viene data rilevanza all'atteggiamento omissivo di Facebook che non ha eliminato i file illeciti, p.50.

[442] §§ 50-51.

[443] Corte Suprema del Wisconsin 30.04.2019, caso n. 2017AP344, Yasmeen Daniel c. Armslist ed altri; opinione dissenziante sul punto da parte del giudice Bradley

[444] ivi, §§ 32-36.

richiedendo la buona fede, si applica a prescindere dallo stato soggettivo, per cui cade ogni possibilità di negarlo a causa del ruolo agevolativo nel compimento del reato[445]: posizione però incompatibile con la disciplina europea, in cui l'elemento soggettivo svolge un ruolo centrale.

In un caso simile (*M.L. v. Craiglist inc.*), invece, l'esito è stato opposto: l'avere Craiglist, con l'architettura del suo sito web, facilitato in vario modo annunci di attività illecite da parte di terzi e ai danni di minore, lo rende content provider e dunque non legittimato al safe harbour ex § 230 CDA (tale invece non è il mero fatto della omessa rimozione, che vi rientra)[446].

25. L'art. 16 c. 3

Il terzo comma, quasi un copia-incolla nel paragrafo 3 della direttiva, prevede che l'autorita' possa esigere dal provider che faccia cessare o che impedisca le violazioni: si è già anticipata qualche riflessione circa l'analoga disposizione contenuta nell'art. 15 c.2. La norma nazionale aggiunge a quella europea che ciò può avvenire anche in via d'urgenza: il che è però superfluo dal momento che, se si ammette l'inibitoria concessa in via definitiva, certamente è ammissibile anche in via d'urgenza. La norma poi è probabilmente superflua anche perché non è autosufficiente, dato che richiede una norma nella sede specifica, che preveda tale potere inibitorio: anche senza la norma de qua, le norme, di cui a tali sedi specifiche, avrebbero

[445] ivi, §§ 34-41: "*This* [sufficienza del *neutral tool* per fruire del § 230 CDA] *is true even when an interactive computer service provider knows, or should know, that its neutral tools are being used for illegal purposes*" (§ 34). La common law permette ad un a. di proporre la tesi, per cui l'applicazione del § 230 CDA è subordinata ad un preliminare verifica (*portal*) di *unconscionability*, ricavata dal ruolo correttivo dello stretto diritto (*textual, black-letter application of the law*) svolto dall'equity: per concedere dunque il safe harbour in caso di risposta negativa (non è stato *unconscionable*, omettendo la rimozione/disabilitazione) e negarlo nel caso di risposta positiva (è stato *unconscionable*, omettendo la rimozione/disabilitazione), giudizio su cui influisce pure il carattere determinato o indeterminato dei soggetti colpiti dall'illecito (così Lin P., *The Portal to Intermediary Liability: Merging Secondary Liability with Equity and Private International Law*, in Wake Forest J. Bus. & Intell. Prop. vol. 20/3, p. 249 ss, spt. sub III).

[446] US District Court-Western District of Washington at Tacoma, 17.04.2020, case No. C19-6153 BHS-TLF, sub Discussion.B.2.b *Craigslist's Immunity From State Law Claims*, p. 22 ss.

continuato a potere operare come prima (non si sarebbe potuto infatti dedurre il contrario dall'istituzione di uno safe harbour del c. 1)[447]. In altre parole poteva essere omessa, dato che nelle sedi specifiche già è contemplato a sufficienza il potere inibitorio e che nei casi, in cui non ci sia norma specifica (problema della inibitoria atipica), non è certo questa la norma che permette di sciogliere il dubbio in senso positivo. Sarà probabilmente stata inserita solo in ossequio al dettato europeo e per mero scrupolo.

Dal dettato si capisce che può trattarsi di una tutela in cessazione, come anche di una tutela preventiva, cioè volta a prevenire future violazioni. Qui il problema principale consiste nel capire quando l'inibitoria è troppo estesa, al punto da costituire quasi un obbligo generale di sorveglianza o di ricerca, vietato dall'articolo 17.

26. L'art. 17 c. 1: la non assoggettabilità ad obbligo generale di sorveglianza o ricerca

L'articolo 17 c. 1 è importante perché pone un principio generale: il provider delle tre tipologie indicate (che possa fruire o meno del safe harbour è irrilevante) non può essere gravato da un obbligo generale di sorveglianza delle informazioni da lui trattate e nemmeno da un obbligo generale di ricerca attiva di fatti che indichino attività illecite[448]. Questa disposizione trova

[447] Ci sarebbe stato semmai il problema di compatibiltià con il divieto di monitoraggio generale ex art. 15 dir. 2000/31 e art. 17 c.1 d. lgs. 70/2003.

[448] In questo scritto la duplice articolazione del principio è per brevità anche espressa con l'espressione "divieto di monitoraggio generale". Quale sia la differenza tra sorveglianza sulle informazioni e ricerca di fatti indicativi di illiceità è difficile dire. Sorvegliare infatti presuppone un qualche scopo per farlo, il quale consisterà -nel contesto specifico- nel cercare (per eventualmente bloccare o rimuovere) materiali illeciti. Del resto anche la sorveglianza deve essere attiva e difficilmente non può essere passiva (intesa questa come rilievo di illiceità solo se me ne sono causalmente imbattuto): una sorveglianza passiva costituisce non tanto un ossimoro, il cui significato sfuggirebbe, ma una *contradictio in terminis*. La differenza tra le due fattispecie del c.1 è dunque assai sottile, se non inesistente. L'una implica l'altra pure secondo M. Husovec, *Injunctions aganist intermediaries*, cit., p. 119, per il quale la prima espressione potrebbe forse riferirsi al divieto di misure passive ed automatiche e la seconda a quelle attive e non automatiche: la proposta tuttavia non persuade, poiché la disposizione non permette di fondare la distinzione sul tipo di strumento (automatico/manuale) usato.

applicazione soprattutto ex post e cioè per le inibitorie che i giudici emanano dopo aver accertato la violazione. L'inibitoria di violazioni future e quindi, dal punto di vista del provider, di caricamenti o permanenze di materiali illeciti futuri, infatti, comporta l'adozione di condotte preventive, che potrebbero richiamare il concetto di sorveglianza o ricerca generale.

Teoricamente il divieto di monitoraggio generale, stando al tenore della disposizione, opera anche ex ante: esclude cioè che la diligenza (non culpa), necessaria per evitare un giudizio di inadempimento o di condotta illecita, possa consistere appunto in un simile monitoraggio. Solo che in tale caso –e limitando il discorso al hosting provider- opera il safe harbour dell'art. 16, per cui lo spazio precettivo dell'art. 17 è in tale caso assai limitato[449]. Però non è inutile, in quanto chiarisce al di là di ogni dubbio che la conoscenza menzionata nell'art. 16 c.1 non è quella che può derivare da un monitoraggio generale: e dunque che la mancata esecuzione di questo non può essere qualificato come conoscenza presunta tale da far perdere il diritto al safe harbour.

Il concetto di sorveglianza/ricerca generale è alquanto vago e qui va criticato il legislatore europeo (meno quello italiano, il quale si sarebbe avventurato in acque perigliose se avesse scelto di precisarlo). Si può andare da un minimo ad un massimo di dovere di sorveglianza/ricerca: ad esempio può concernere qualunque violazione da qualunque fonte[450] e di qualunque diritto oppure può limitarsi alle semplici violazione del diritto d'autore su una certa opera dell'ingegno e provenienti da una determinata fonte sostanziale o magari addirittura solamente da un certo server (numero IP). Se intesa nel senso più ampio, non ci sarà probabilmente alcuna inibitoria che la violerà: in causa il soggetto leso chiederà infatti il monitoraggio completo ma solo sui file che costituiscano violazione della propria opera portata sub iudice. Però un significato così ampio non è sensato

[449] Tosi E., *La disciplina applicabile all'hosting provider*, cit., 249, dice qualcosa di analogo, quando scrive di assenza di un obbligo di sorveglianza "preventivo", dato che viene meno dopo la *notitia criminis*.

[450] Da qualunque domain name, da qualunque numero IP etc. Le inibitorie possono riferirsi al blocco del numero IP, del nome di dominio oppure ad una URL (Lodder A.R.-Polter P., *ISP blocking and filtering: on the shallow justification in case law regarding effectiveness of measures*, in *European Journal of Law and Technology*, vol. 8/2, 2017, § 4.1).

attribuirlo alla normativa, dal momento che nessuno può pensare che gravi sul provider un dovere di vigilanza su tutto.

Il problema si porrà magari in relazione alla latitudine dell'inibitoria circa una violazione su una specifica opera dell'ingegno: è qui che ci si chiede quando ricorra l'obbligo generale di sorveglianza o ricerca. Per quanto si restringa la portata del concetto de quo, potrebbe ritenersi che non lo violasse l'inibitoria per la prevenzione della violazione di una sola opera protetta, anche se da qualunque fonte provenga: si tratterebbe infatti di applicazione della regola di liceità della sorveglianza quando ricorrono "casi specifici" (cons. 47)[451].

In senso contrario potrebbe però dirsi che l'obbligo generale di sorveglianza o ricerca, vietato ex art. 17 c. 1 d. lgs. 70, fosse quello emergente da una lite determinata, il che presuppone l'allegazione di una specifica (o anche più, ma determinate) violazione e cioè di diritti ben individuati: una specifica opera dell'ingegno, uno specifico diritto di marchio, uno specifico fatto diffamante o lesivo della riservatezza, causato da una specifica fonte. Un divieto generale ed astratto costituirebbe in pratica quasi norma di legge, mentre il comando giudiziale è sempre relativo ad una specifica lite. Pertanto, dovendosi riferire il divieto di obbligo generale di sorveglianza o ricerca ex art. 17 c. 1 d. lgs. 70 ad una specifica lite, potrebbe sostenersene un'interpretazione nel senso che il dovere di monitoraggio, anche se riferito ad una specifica violazione (uno specifico diritto d'autore, uno specifico fatto diffamatorio), non può riguardare tutti i file presenti e futuri sui server del provider.

27. (segue:) la sentenza Scarlet. Rilevanza dello stato della tecnologia

Questo è sostanzialmente l'esito di C.G. 24.11.2011, C-70/10, Scarlet Extend c. SABAM, secondo cui: la dir. 31/2000 oltre a dir. 2001729 e dir. 2004 /48 e a quella sulla tutela della riservatezza <<*ostano ad un'ingiunzione rivolta ad un fornitore di accesso ad Internet di predisporre un sistema di filtraggio: – di tutte le comunicazioni elettroniche che transitano per i suoi*

[451] Per quanto si dovrebbe chiarire l'uso del termine "regola" per un *Considerando*, che è solo illustrativo del precetto posto dall'articolato. Anche questa è comunque una regola inutile: se il divieto riguarda la sorveglianza generale, è ovvio che il il dovere di sorveglianza per casi specifici fuoriesce da tale divieto.

servizi, in particolare mediante programmi «peer-to-peer»; – che si applica indistintamente a tutta la sua clientela; – a titolo preventivo; – a sue spese esclusive, e – senza limiti nel tempo, idoneo ad identificare nella rete di tale fornitore la circolazione di file contenenti un'opera musicale, cinematografica o audiovisiva rispetto alla quale il richiedente affermi di vantare diritti di proprietà intellettuale, onde bloccare il trasferimento di file il cui scambio pregiudichi il diritto d'autore>>. Infatti una simile ingiunzione <<*obbligherebbe … il fornitore a prestare una sorveglianza attiva su tutti i dati di ciascuno dei suoi clienti per prevenire qualsiasi futura violazione di diritti di proprietà intellettuale, costringendolo in tal modo ad effettuare una sorveglianza generalizzata, che è vietata dall'art. 15, n. 1, della direttiva 2000/31. Essa comporterebbe inoltre una grave violazione della libertà di impresa del fornitore di cui trattasi, poiché l'obbligherebbe a predisporre un sistema informatico complesso, costoso, permanente e unicamente a suo carico, il che risulterebbe peraltro contrario alle condizioni stabilite dall'art. 3, n. 1, della direttiva 2004/48, il quale richiede che le misure adottate per assicurare il rispetto dei diritti di proprietà intellettuale non siano inutilmente complesse o costose. Pertanto, siffatta ingiunzione non rispetterebbe l'esigenza di garantire un giusto equilibrio tra, da un lato, la tutela del diritto di proprietà intellettuale, di cui godono i titolari dei diritti d'autore, e, dall'altro, quella della libertà d'impresa, appannaggio di operatori come i fornitori di accesso a Internet. Gli effetti di detta ingiunzione, tra l'altro, non si limiterebbero a colpire tali fornitori, poiché il sistema di filtraggio è idoneo a ledere anche i diritti fondamentali dei clienti, ossia il loro diritto alla tutela dei dati personali e la loro libertà di ricevere o di comunicare informazioni, diritti, questi ultimi, tutelati dagli artt. 8 e 11 della Carta dei diritti fondamentali dell'Unione europea. Da un lato, l'ingiunzione implicherebbe un'analisi sistematica di tutti i contenuti, nonché la raccolta e l'identificazione degli indirizzi IP degli utenti all'origine dell'invio dei contenuti illeciti sulla rete, indirizzi che costituiscono dati personali protetti, in quanto consentono di identificare in modo preciso i suddetti utenti. Dall'altro, rischierebbe di ledere la libertà di informazione, poiché tale sistema potrebbe non essere in grado di distinguere adeguatamente tra un contenuto lecito ed un contenuto illecito, sicché il suo impiego potrebbe produrre il*

risultato di bloccare comunicazioni aventi un contenuto lecito>>[452].

La soluzione del problema dipende prevalentemente dallo stato di avanzamento della tecnologia[453] (il che comprende pure il profilo degli errori, inevitabili allo stato attuale, anche se non è chiaro in che misura lo siano[454]). La disposizione mirava infatti a non caricare di doveri eccessivi questa attività, allo stato allora nascente, ritenuta assai importante: si intuiva infatti che le attività economiche si sarebbero svolte sempre più on line. Ora il giudizio di tollerabilità del dovere di prevenzione dipende dai mezzi a disposizione: più sono disponibili ed efficaci i mezzi (filtri), più estesa può diventare l'attività di sorveglianza esigibile. Si dovrebbero dunque considerare i mezzi disponibili astrattamente e concretamente in un certo momento storico: astrattamente, nel senso di soluzioni disponibili sul mercato (non quelle ancora allo stato di ricerca o prima sperimentazione); concretamente, nel senso di pretendibili in base al loro costo rapportato alle dimensioni dell'impresa di internet providing (tale duplice articolazione costituisce il giudizio di diligenza, sia contrattuale sia –in negativo cioè come non culpa- aquiliana)[455].

[452] Ho riportato le massime ufficiali: per il testo v. §§ 40, 48-52 e dispositivo. In dottrina v. in tale senso Falletta P., *Controlli e responsabilità dei social network sui discorsi d'odio online*, cit., 153.

[453] La quale, evolvendo, è normale determini difficoltà applicative del diritto. Ad es. i file scambiati col protocollo BitTorrent tramite server veloci affittati (virtual private servers: VPS), stante l'architettura di questo tipo di file sharing p2p (frammentazione del file in chunks inviati da server diversi) non possono essere intercettati algoritmicamente su un singolo server. Per cui la responsabilità dei titolari di VPS sorge solo in base ad *actual knowledge* (§ 512.c.1.A.i § 512 DMCA) causata da specifica diffida (notice) dei copyright holders (Wang S.J., *DMCA Safe Harbors for Virtual Private Server Providers Hosting BitTorrent Clients*, 12 *Duke Law & Technology Review* 163-181 (2014), 176).

[454] Keller D., *Internet Platforms: Observations on Speech, Danger, and Money*, cit., scrive di un tasso di accuratezza del 70/80 per cento per il *natural language processing* e per la *sentiment analysis*.

[455] Si v. il § 5 dell'art. 17 dir. 2019/790 di modifica del copyright: <<*per stabilire se il prestatore di servizi si è conformato agli obblighi di cui al paragrafo 4 e alla luce del principio di proporzionalità, sono presi in considerazione, tra gli altri, gli elementi seguenti: a) la tipologia, il pubblico e la dimensione del servizio e la tipologia di opere o altri materiali caricati dagli utenti del servizio; e b) la disponibilità di strumenti adeguati ed efficaci e il relativo costo per i prestatori di servizi*>>. Si è ricordato sopra che Facebook vaglia praticamente tutto quanto passa sulla sua piattaforma (Gorwa R.-Bins R.-Katzenbach C., *Algorithmic content moderation: Technical and political challenges*, cit., p. 9): se così è, in

Verosimilmente questo aspetto non era presente al legislatore europeo del 2000, il quale non conosceva i filtri automatici in base a parametri impostati e continuamente modificabili. Tuttavia, da un lato, il giudizio di illiceità è spesso gravato da un'insopprimibile area di soggettività e, dall'altro, i software di filtraggio spesso sbagliano, come detto (da vedere se nel senso sia di falsi positivi che di falsi negativi). Resta fermo, però, che il giudizio sull'inammissibile genericità/ammissibile specificità del controllo pretendibile dipende largamente dalla tecnologia a disposizione[456].

28. Una recente opinione dell'A.G. presso la C.G. in causa c-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland limited*

E' stato osservato che, senza il divieto ex art. 15 dir. 2000/31 (letteralmente: se uno Stato membro potesse imporre un obbligo generale di sorveglianza)[457], l'host provider: 1) potrebbe perdere l'immunità di prestatore intermediario, poiché non sarebbe più neutro. Infatti non conserverebbe il suo carattere tecnico, automatico e passivo, il che implicherebbe che detto host provider sarebbe al corrente delle informazioni memorizzate ed eserciterebbe un controllo sulle medesime. 2) Inoltre, anche qualora tale rischio non esistesse, potrebbe, in linea di principio, essere ritenuto responsabile di qualsiasi attività o informazione illecita, senza che le condizioni enunciate all'articolo 14, paragrafo 1, lettere a) e b), di tale direttiva siano effettivamente

tale caso la questione del monitoraggio generale diviene sostanzialmente irrilevante, almeno sotto il profilo tecnologico e potrebbe portare ad una disapplicazione della norma con interpretazione evolutiva. Il problema diventerebbe allora quello di riuscire a dare prova di ciò.

[456] <<*A tale stregua, benché, al fine di favorire la diffusione dei servizi della società dell'informazione e i vantaggi ad essa collegati, anche l'hosting provider attivo va esonerato da obblighi preventivi e generalizzati di monitoraggio, nondimeno, qualora la tutela dei diritti di proprietà intellettuale può avvenire in modo efficace adeguato attraverso gli strumenti tecnologici a disposizione dell'hosting provider sulla base delle informazioni fornite dallo stesso titolare del diritto violato, non vi è più alcuna ragione per esimere ulteriormente l'hosting provider, affiancandolo dal rispetto dei diritti di proprietà intellettuale che oggettivamente concorre a violare*>>: Trib. Roma 10.01.2019 RTI c.Vimeo, Rg 23732/2012, p. 24.

[457] Tuttavia le due affermazioni non sono specularmente opposte: si può infatti immaginare l'assenza sia del divieto ex art. 15 dir. 2000/31, sia –almeno come assenza espressa- dell'obbligo di monitoraggio generale.

soddisfatte. È vero, prosegue questa opinione, che l'articolo 14, paragrafo 1, lettera a), della direttiva 2000/31 subordina la responsabilità [rectius: l'esenzione da responsabilità] di un prestatore intermediario alla conoscenza effettiva dell'attività o dell'informazione illecita. Tuttavia, alla luce di un obbligo generale in materia di sorveglianza, si potrebbe ritenere che il carattere illecito di qualsiasi attività o informazione venisse portato "d'ufficio" a conoscenza di tale prestatore intermediario e che quest'ultimo dovrebbe procedere alla rimozione di tali informazioni o disabilitare l'accesso alle medesime, senza che esso abbia compreso il contenuto illecito. Di conseguenza, si prosegue, la logica dell'immunità relativa in materia di responsabilità per le informazioni memorizzate da un prestatore intermediario sarebbe sistematicamente sovvertita: il che arrecherebbe pregiudizio all'effetto utile dell'articolo 14, paragrafo 1, della direttiva 2000/31. In conclusione, per il <<*combinato disposto dell'articolo 14, paragrafo 3, e dell'articolo 15, paragrafo 1, della direttiva 2000/31 che un obbligo imposto ad un prestatore intermediario nell'ambito di un'ingiunzione non può avere come conseguenza che, rispetto alla totalità o alla quasi totalità delle informazioni memorizzate, il ruolo di tale prestatore intermediario non sia più neutro nel senso descritto al paragrafo precedente*>>[458].

Circa questa presa di posizione teorica del bravo AG Szpunar su uno dei temi più complessi della platform liability/accountability/responsibility, si possono muovere delle osservazioni[459]. Circa 1), il ruolo neutro automatico e passivo riposa solo sul cons. 42, che cede di fronte al dettato dell'art. 14 e comunque è riferito solo ai primi due tipi di provider (art. 12-13), non all'hosting provider ex art. 14, come detto sopra. Circa sub 2) (non chiarissimo), è vero che il dovere di sorveglianza estesa sarebbe probabilmente incompatibile con l'art. 14/1 dir. (se ben capisco). Quest'ultimo vuole che non ci sia responsabilità per i contenuti caricati, fino a che il provider non sappia oppure, se sa, qualora abbia proceduto a rapida rimozione/disabilitazione. La violazione di un dovere di

[458] Conclusioni AG Szpunar 04.06.2019, C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, §§ 35-40.

[459] Da prendere con cautela, dato che il ragionamento condotto dal'AG è un po' astatto e dunque complesso.

sorveglianza, invece, potrebbe esporlo a qualche responsabilità in uno stadio a monte e cioè anche senza e prima che egli sapesse: in questo senso una così ipotizzata norma nazionale probabilmente sarebbe incompatibile con l'art. 14/1 dir. 2000/31. Si potrebbe superare il problema, intendendo opportunamente l'ipotizzato dovere di sorveglianza generale e cioè secondo la diligenza esigibile da operatori professionali eiusdem condicionis et professionis (come si dovrebbe in realtà fare, non potendosi immaginare posizioni di garanzia). E' dunque errato dire con l'AG che in tale ipotesi <<*il carattere illecito di qualsiasi attività o informazione venga [verrebbe] portato d'ufficio*[460] *a conoscenza di tale prestatore intermediario e che quest'ultimo dovrebbe procedere alla rimozione di tali informazioni o disabilitare l'accesso alle medesime, senza che esso abbia [avesse] compreso il contenuto illecito*>>. Il canone di diligenza escluderebbe di certo tale scenario: non potrebbe ritenersi il provider "notiziato" per il solo dovere astratto di sorvegliare, ma semmai dopo esame delle circostanze e dopo prova che egli, tramite appositi filtri disponibili sul mercato, avrebbe potuto sapere (prova assai difficile per la segretezza che ricopre queste tecnologie). Il problema di compatibilità con l'art. 14 sarebbe altro: l'equilibrio di interessi, composto da quest'ultima norma, prevede che il provider non possa essere censurato per negligente controllo ex ante dei materiali ospitati e tocchi invece al soggetto leso segnalarglieli. In altre parole il provider può comunque stare tranquillo, fino a che non riceva una specifica segnalazione, senza preoccuparsi di setacciare le migliaia/i milioni di file ospitati: <<il punto di equilibrio è stato allora rinvenuto in un sistema di controllo successivo e ad attivazione precipua da parte del soggetto titolare dei diritti d'autore ritenuti violati.>>[461]. Con questa disciplina allora contrasterebbe un

[460] L'espressione "d'ufficio" (§ 38 delle Conclusioni) mi pare da intepretare come "automaticamente" (automatically, zwangsläufig, d'office, de oficio in alcune altre lingue): cioè conoscenza presunta *iure et de iure*, diremmo meglio.

[461] Così Trib. TO 07.04.2017, Delta ITV Broadcasting c. TVCatchup c. Google – Youtube, RG 38112/2013, sub 6.1, p. 21. Si tratta di posizione largamente diffusa. Tuttavia nel diritto d'autore (fonte prevalente delle violazioni) questo equilibrio è oggi diventato poco soddisfacente, a causa dell'imprevisto ed ubiquo moltiplicarsi della c.d. pirateria digitale (Slabykh I., *The New Approaches to Digital Anti-Piracy in the Entertainment Industry*, 19 UIC *Rev. Intell. Prop. L-J.Marshall Law School*. 75 (2019), sub II.B, 85 ss.). In Europa l'industria culturale

ipotetico obbligo generale di sorveglianza o ricerca, sia ex ante sia dopo ingiunzione: anche in quest'ultimo caso infatti opera il divieto ex art. 15 § 1 dir. 2000/31-art.17 c. 1 d. lgs. 70/2003, come si evince dalla giurisprudenza sopra ricordata. Ne segue che queste due norme probabilmente sono a stretto rigore inutili: anche senza di esse, un obbligo generale di sorveglianza o ricerca (a livello di comando generale es astratto –legge- o specifico e concreto –inibitoria-) sarebbe comunque in contrasto con l'art. 14/1 dir. 2000/31.

Si tratta di un equilibrio come tanti altri e non è detto che rimanga a lungo così. Si v. ad es. la nuova dir. 2019/790 di riforma del copyright in cui la posizione del provider è aggravata (quasi rovesciata), dato che egli è responsabile (in proprio, pare) per violazione del diritto di comunicazione al pubblico, a meno che provi il ricorrere delle esimenti di legge[462]. Anche se potrebbe dirsi l'opposto e cioè che, una volta accontentati i più forti economicamente tra i titolari dei diritti più spesso violati in internet (copyright), la modifica della dir. 2000/31 è diventata meno urgente[463].

Al momento, è probabilmente esatta la corrente opinione,

(musicale, essenzialmente) è riuscita a conseguire un risultato importante tramite l'art. 17 della nuova dir. copyright 790/2019.

[462] Dir. 2019/790 del 17.04.2019, art. 17, §§ 1-3-4. Si è così tentato di riparare al c.d *value gap* e cioè all'(asserita) iniqua distribuzione dei profitti traibili dagli usi online che, soprattutto per l'operare del safe harbour, andrebbero alle piattraforme e non –o non sufficientemente- ai titolari dei diritti (mancherebbero però dati empirici a conferma: Frosio G., *Reforming the C-DSM Reform: A User-Based Copyright Theory for Commonplace Creativity* (November 14, 2019), *Centre for International Intellectual Property Studies (CEIPI)*, Research Paper No. 2019-12, p. 12-13, letto in ssrn.com). Che tale *value gap* esista, però, è contestato, dati alla mano, ed anzi l'abolizione del safe harbour (v. dir. UE 790/2019, art. 17 per il diritto d'autore), chiesta soprattutto dall'industria culturale, potrebbe paggiorarne la situazione economica: così l'analitico lavoro di Elkin Koren N.–Nahmias Y.– Perel M, *Is It Time to Abolish Safe Harbor? When Rhetoric Clouds Policy Goals*, di prossima pubblicazione in *Stanford Law & Policy Review*, Last revised: 2 Jun 2019, letto in ssrn.com (parte III, 16 ss. e IV39 ss). Il termine *value gap* è usato anche per esprimere diverso concetto e cioè quello della non coestensione (simmetrica) tra safe harbour e responsabilità: nel senso che può capitare che certi provider perdano il diritto al primo, senza però ricadere nella seconda (Nordemann J.B., *Liability of online service providers for copyrighted content-Regulatory action needed?*, gennaio 2018, p 21). Il che però è normale, se si accetta che si tratti di "esimenti".

[463] Ma non dovrebbe essere così. L'inizio dei lavori a livello europei sul Digital Services Act (v. infra) fa pensare ad una modifica della dir. 2000/31.

secondo cui, nella scelta tra il keep up (disattendendo le ragioni del soggetto leso, quindi con possibile responsabilità verso costui) e il take down (accogliendo le ragioni medesime, quindi con possibile responsabilità verso l'utente uploader), il provider continuerà probabilmente ad optare per la seconda via, procedendo a rimozione/disabilitazione[464] (sono stati già rilevati frequenti abusi della richiesta di take down, soprattutto nei rapporti tra imprese concorrenti[465]).

29. L'inibitoria. Giurisprudenza europea in tema

La giurisprudenza, europea e nazionale, è intervenuta su questi aspetti.

La premessa è che sia possibile imporre inibitorie ad intermediari, anche se questi non sono responsabili della violazione[466]. Questo è pacificamente desumibile dagli artt. 11 dir. 48/2004 e dall'art. 8 c. 3 dir. 29, dal contenuto del tutto analogo[467]: qui è chiara la contrapposizione tra provvedimenti contro gli autori della violazione (art- 8 c- 2) e provvedimenti contro gli intermediari utilizzati (art. 8 c. 3). Ed è chiaro pure in base alla struttura degli artt. 12-13-14 dir. 31/2000, i cui § 3 distinguono la responsabilità dalla soggezione ad inibitoria. Nel

[464] V. Conti G.L., *Manifestazione del pensiero attraverso la rete e trasformazione della libertà di espressione: c'è ancora da ballare per strada?*, Riv. AIC, 2018/4, 212; Donati F., voce *Internet (diritto costituzionale)*, Enc. dir., Annali, VII, 2014, Giugffrè, § 6: <<*Di fatto poi gli intermediari sono portati, in caso di dubbio, a privilegiare un intervento "censorio" rispetto ad una decisione che potrebbe esporli ad azioni risarcitorie da parte dei soggetti lesi: interventi del genere finiscono evidentemente per ledere la libertà di informazione del soggetto che ha immesso in rete il contenuto censurato o di coloro che avrebbero interesse a conoscerlo*>. Viene così attuata quella che è stata chiamata *collateral censorship* (censura delegata) o *digital prior restraint* (censura pretentiva) da Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, in *UC Davis Law Review* vol. 51, 3, february 2018, 1149 ss, sub II.B, p. 1172 ss.

[465] Keller D., *Internet Platforms: Observations on Speech, Danger, and Money*, cit., 26/7.

[466] Tra le molte decisioni lo esplicitano: C.G. *L'Oreal ed altri c. eBay*, 12.07.2011, C-324/09, § 128-134; C.G. 07.07.2016, *Tommy Hillfiger*, C-494/5, § 22; C.G. 03.10.2019, *Eva Glawischnig-Piesczek c. Facebook*, C-18/18, § 25, richiamandosi al § 32 delle Concluisioni dell'A.G. 04.06.2019 nella stessa causa. In Italia v. ad es. Trib. MI 12.4.18, *Mondadori c. Fastweb ed altri*, § 9-10.

[467] Conf. AG Szpunar nelle conclusioni 08.02.2017, Stichting Brein c. Ziggo, C-610/15, § 56.

diritto interno si v. l'art. 156 c. 1 l. aut. e 163/1 l. aut. nonché art. 124 c. 1 c.p.i. (inibitoria definitiva) e art. 131 c. 1 ult. parte c.p.i.. (inibitoria cautelare). Che la soggezione all'inibitoria prescinda da un titolo di (cor-)responsabilità risarcitoria, è pacificamente accettato dalla dottrina[468].

Come sopra anticipato, tuttavia, quanto appena detto non vale più –o non negli stessi termini- con la dir. 790 del 2019 sulla riforma del diritto d'autore. Questa dispone d'imperio che: - da un lato <<(..) il prestatore di servizi di condivisione di contenuti online effettua un atto di comunicazione al pubblico o un atto di messa a disposizione del pubblico ai fini della presente direttiva quando concede l'accesso al pubblico a opere protette dal diritto d'autore o altri materiali protetti caricati dai suoi utenti.>> (art. 17/1); - dall'altro, che in tale caso non opera il safe harbour ex art. 14/1 della dir. 2000/31[469] (art. 17/3). Il semplice ospitare[470] file illeciti costituisce violazione del diritto di autore: a meno che ricorrano o un titolo negoziale o un'elevata diligenza ex ante (filtraggio) o ex post (rimozione/disabilitazione) (art. 17/4)[471]. Ma su questa importante novità e le sue implicazioni sistematiche non si può qui dire di più[472]. Tuttavia la pressione concorrenziale –e accordi stipulati all'ombra del DMCA tra le piattaforme e le major dell'industria culturale- hanno fatto si che anche negli USA, pur mancando ad oggi nel DMCA del 1998

[468] Rosati E., *Copyright and the Court of Justice*, Oxford University press, 2019, 155. V. poi i lavori di Husovec M., ad es.: *Asking innocent third parties for a remedy*, in Hofmann F.-Kurz F. (eds.), *Law of remedies. A European perspective*, Intersentia, 2019. 237; spt. la sua monografia Husovec M., *Injunctions aganist intermediaries in the European Union. Accountable but not liable?*, cit., incentrata –come già il titolo suggerisce- proprio su questo (v. spt. cap. 4.2, p. 57 ss).

[469] Che la dir. 790 chiama "limitazione di responsabilità" invece che "esenzione", come sarebbe stato più appropriato.

[470] Nonché il mettere on line: ma questo è ovvio, trattandosi della attività propria di chi presta servizi internet di "condivisione". Il semplice hosting, senza messa on line pubblica, costituisce cloud storage o servizi simili (v. definizione all'art. 2 n. 6).

[471] La quale avviene, oltre che su segnalazione/difffida dell'interessato, su segnalazione di qualsiasi altro utente della piattaforma (community flagging).

[472] V. Albertini L., *La modifica al diritto d'autore europeo per tener conto del contesto digitale: note sugli artt. 11 (diritto degli editori) e 13 (responsabilità dei provider) della bozza di direttiva UE nel febbraio 2019, uscita dalla fase c.d. trilogue*, in medialaws.eu, Law and Media Working Paper Series No. 2/2019, spt. §§ 6 ed 8..

una disciplina restrittiva come il cit. art. 17 dir. 2019/790, le piattaforme adottassero ugualmente filtri automatici: le grosse imprese titolari di copyright, infatti, sostenevano che non provvedere in tale senso sarebbe stato qualificabile come trarre beneficio dalle (ed anzi agevolare le) violazioni[473].

Torniamo ora alla giurisprudenza sul punto.

la Corte di Giustizia 12 luglio 2011, L'Oreal c. eBay, non è particolarmente interessante, anche se spesso citata. Al § 142 dice che si può ingiungere al gestore di un mercato online di adottare misure che consentono di agevolare l'identificazione dei suoi clienti venditori e non può essere opposta la privacy: <<*a tal proposito, come ha giustamente esposto la L'Oréal nelle sue osservazioni scritte e come risulta dall'art. 6 della direttiva 2000/31, se è certamente necessario rispettare la protezione dei dati personali, resta pur sempre il fatto che, quando agisce nel commercio e non nella vita privata, l'autore della violazione deve essere chiaramente identificabile*>>[474]. Successivamente chiarisce l'ovvio e cioè che, secondo l'articolo 11, 3° per., direttiva 48/2004, si può ingiungere al mercato online eBay non solo di far cessare le violazioni, ma anche di prevenire nuove violazioni della stessa natura (§ 144)[475].

Ad onore del vero, curiosamente l'articolo 11, terzo per., dir. 48 non specifica il contenuto dell'ingiunzione verso gli intermediari: ma questo è superabile, dato che andrà interpretato come nel primo periodo nell'articolo, laddove la riferisce all'autore della violazione e dunque un ordine di cessazione del proseguimento della violazione. Inoltre in questa prima parte dell'art. 11 l'ingiunzione è solamente di cessazione e non menziona l'astensione da condotte future. In questo senso allora

[473] Sag M., *Internet Safe Harbors and the Transformation of Copyright Law*, cit., sub II.A e II.B, 538 ss, che chiama il fenomeno *DMCA-plus*. Infatti per il § 512 DMCA il ricevere <financial benefit directly attributable to the infringing activity> osta al safe harbour: sub (c)(1)(B) e sub (d)(2). I titolari di copyright,. del resto, sono stati i più abili a forgiare lo sviluppo dell'internet a loro favore (Suzor N.P., *Lawless. The secret rules that govern our digital lives*, cit., p. 59-60; v. poi p. 70 ss).

[474] E' la causa C-324/09.

[475] La cosa non è in discussione dato che addirittura è ammessa l'inibitoria anche prima che si verifichi un danno (ex multis v. Di Majo A., *La tutela civile dei diritti.3*, terza ed., Giuffrè, 2001, 143 ss.) e per alcuni anche prima che si verifichi un illecito (contrario però Nardo G.N., *Profili sistemtici dell'azione civile inibitoria*, ESI, 2017, p. 90).

può ravvisarsi uno spunto interpretativo utile nella menzionata sentenza della Corte di Giustizia, anche se la cosa non era dubbia: l'inibitoria de futuro è espressamente menzionata nell'art. 18 § 1 dir. 31/2000 e nel c. 3 degli artt. 12-13-14 della stessa[476], oltre che –ma questo ha scarso valore ermeneutico- dal cons. 24 della dir. 2004/48[477]. Del resto non si può pensare che la Direttiva del 2004 le abbia abrogate, essendo disposizioni espressamente fatte salve dall'art. 2 §§ 2-3 dir. 48/04-; né si vedono ragioni per una portata dell'inibitoria nella proprietà intellettuale più ristretta di quella propria della inibitoria nell'illecito civile comune (cioè che preveda solo la cessazione e non la prevenzione). La dottrina concorda nell'ammettere la generalità dell'inibitoria preventiva verso gli intermediari[478].

Ci sono poi due sentenze nel biennio 2011-2012 con medesimo relatore, medesimo A.G. e medesimo attore originario (SABAM, collecting del Belgio), che son di qualche interesse.

Nella prima (Scarlet Extended c. SABAM)[479] l'azione è proposta contro un fornitore di accesso[480] tramite il quale venivano scambiati file illeciti per mezzo di un software peer to peer. Nella seconda (Sabam c. Netlog)[481] l'azione è proposta contro una piattaforma belga di social network (poi chiuso), tramite la quale pure venivano scambiati file illeciti, rappresentanti opere del repertorio attoreo[482]. Le domande

[476] Anche l'art. 8 dir. 29 si limita a parlare di ingiunzioni, senza alcun riferimento alla condotta oggetto di provvedimento inibitorio.

[477] Nel senso dell'ammissibilità di inibitorie in prevenzione, oltre che di cessazione,. v. C.G. 24.11.2011, *Scarlet Extended c. SABAM*, C-70/10, § 31 (invocando *L'Oreal contro eBay*, C-324/09), e C.G. 16.02.2012, *Sabam c. Netlog*, C-360/10, § 29 (invocando Scarlet Extended c. SABAM: sono frequenti i richiami solo tralatizi nella giurisprudenza della Corte). C'è però da precisare il concetto di prevenzione: prevenzione ma pur sempre dopo un illecito (magari produttivo di danno) o ancbhe prima che si verifichi qualunque illecito (si pensi alle azioni di nunciazione, artt. 1171-1172 c.c.)? questo è il dubbio più significativo.

[478] Rosati E., *Copyright and the Court of Justice*, cit., 157/8.

[479] C.G. 24.11.2011, *Scarlet Extended c. SABAM*, C-70/10.

[480] così almeno si legge (§ 16) e a conferma son richiamati in premesse gli artt.12 e 15 dir. 31/2000, non gli artt. 13 e 114.

[481] C.G. 16.02.2012, *Sabam c. Netlog*, C-360/10.

[482] Si trattava di hosting provider: è infatti richaiamato l'art. 14 dir. 31/2000: v. poi il § 27..

pregiudiziali sono simili[483] e consistono nel capire se l'inibitoria può consistere in un sistema di filtraggio preventivo su tutti i file transitati o memorizzati dai due provider e per tutti i clienti, senza limiti di tempo e a spese del provider.. La risposta della C.G. è che il diritto europeo osta ad una simile ingiunzione[484]. Infatti <<*una simile ingiunzione obbligherebbe il suddetto prestatore a procedere ad una sorveglianza attiva della quasi totalità dei dati relativi a ciascuno degli utenti dei suoi servizi, onde prevenire qualsiasi futura violazione di diritti di proprietà intellettuale, imponendogli in tal modo una sorveglianza generalizzata vietata dall'articolo 15, paragrafo 1, della direttiva 2000/31. Essa causerebbe, peraltro, una grave violazione della libertà di impresa del prestatore di servizi di hosting, poiché l'obbligherebbe a predisporre un sistema informatico complesso, costoso, permanente e unicamente a sue spese, il che risulterebbe peraltro contrario alle condizioni stabilite dall'articolo 3, paragrafo 1, della direttiva 2004/48, il quale richiede che le misure adottate per assicurare il rispetto dei diritti di proprietà intellettuale non siano inutilmente complesse o costose. Pertanto, un'ingiunzione siffatta non rispetterebbe l'esigenza di garantire un giusto equilibrio tra, da un lato, la tutela del diritto di proprietà intellettuale, di cui godono i titolari di diritti d'autore, e, dall'altro, quella della libertà d'impresa, di cui beneficiano operatori quali i prestatori di servizi di hosting. Gli effetti di una simile ingiunzione non si limiterebbero, del resto, al prestatore di servizi di hosting, poiché il sistema di filtraggio è idoneo a ledere anche i diritti fondamentali degli utenti dei medesimi, ossia il loro diritto alla tutela dei dati personali e la loro libertà di ricevere o di comunicare informazioni, diritti, questi ultimi, tutelati dagli articoli 8 e 11 della Carta dei diritti fondamentali dell'Unione europea. Da un lato, l'ingiunzione implicherebbe l'identificazione, l'analisi sistematica e l'elaborazione delle informazioni relative ai profili creati sulla rete sociale dagli utenti della medesima, informazioni, queste, che costituiscono dati personali protetti, in quanto consentono, in linea di principio, di identificare i suddetti utenti. Dall'altro, essa rischierebbe di ledere la libertà di informazione, poiché tale*

[483] V. § 28 e, rispettivamente, § 25.

[484] V. il dispositivo della sentenza.

sistema potrebbe non essere in grado di distinguere adeguatamente tra un contenuto illecito ed un contenuto lecito, sicché il suo impiego potrebbe produrre il risultato di bloccare comunicazioni aventi un contenuto lecito>>[485].

In sintesi, bilanciando gli interessi coinvolti (diritto violato portato in giudizio, liberta di impresa del provider, diritto dell'utente alla riservatezza, diritto dell'utente di informazione attivo e passivo[486]), la Corte ha sciolto il dubbio, affermando che simile comando inibitorio: i) viola il divieto di monitoraggio generale; e ii) impone misure inutilmente complesse e costose (art. 3/1 dir. 2004/48). Dal fraseggio della motivazione (prendiamo Sabam c. Netlog, C-360/10), sembrano essere invocati entrambi i motivi di incompatibilità, essendoci due esami e due conclusioni (§ 38 e § 51), anche se ne sarebbe probabilmente bastato uno solo. La C.G. non chiarisce il rapporto tra questi due limiti, gravanti sui doveri imponibili al provider: si può però dire che l'art. 3 dir. 2004/48 abbia generalizzato il criterio sottostante al divieto di monitoraggio generale ex art. 15 § 1 dir. 2000/31.

Pure interessante è la sentenza nel caso UPC Telekabel c. Constantin Film-Wega Filmproduktions del 27 marzo 2014[487]. Qui la questione pregiudiziale era la seguente: <<*Se sia compatibile con il diritto dell'Unione, in particolare con la necessità di operare un bilanciamento fra i diritti fondamentali delle parti coinvolte, vietare a un fornitore di accesso [a Internet] in modo totalmente generale (dunque senza la prescrizione di misure concrete) di consentire ai suoi abbonati l'accesso a un determinato sito Internet fintanto che in quest'ultimo siano, esclusivamente o prevalentemente, resi accessibili contenuti senza l'autorizzazione del titolare dei diritti, qualora il fornitore di accesso [a Internet] possa evitare sanzioni per la violazione di tale divieto dimostrando di avere comunque adottato tutte le misure ragionevoli* >> (§ 17 sub 3).

[485] Massima ufficiale di *Sabam c. Netlog*, C-360/10, che rinvia ai §§ 38, 46-50 e 52 della sentenza.

[486] Ma allora anche il diritto dei destinatari dell'upload a ricevere informazioni da quell'utente e a trasmettergliele.

[487] C.G. 27.03.2014, C-314/12. Il fatto (§ 11): due produttori cinematografici si accorgono che un sito ospita possibilità di vedere in streaming film da loro prodotti e chiedono che sia emessa ingiunzione di bloccco dell'accesso ad internet a carico del provider di accesso ad internet UPC Telekabel Wien.

E la risposta è positiva in relazione alla libertà di impresa, dato che il destinatario può scegliere le misure più adatte e comunque può sottrarsi al responsabilità dimostrando di aver adottato tutte le misure ragionevoli (§§ 51-53). Quanto alla libertà di informazione degli utenti Internet, bisogna che le norme nazionali prevedono la possibilità di ricorrere contro le misure adottate dal provider (§ 57). Per quanto riguarda il terzo interesse in conflitto (la proprietà intellettuale, cioè il diritto leso), il giudice ammette che un'inibitoria di questo tipo possa non essere risolutiva e cioè che possa far filtrare eventuali future violazioni: eventualità però non anomala, ricorda la Corte, poiché il diritto d'autore non è sempre e comunque prevalente sugli altri diritti[488]. E' allora sufficiente che la misura adottata abbia l'effetto di impedire o rendere difficilmente realizzabili le consultazioni non autorizzate. Perché poi vi sia un giusto bilanciamento tra i vari diritti coinvolti, bisogna che la misura non privi inutilmente gli utenti di internet della possibilità di accedere in modo lecito alle informazioni disponibili: in pratica, che sia un inibitoria mirata cioè con oggetto sufficientemente preciso (§§ 61-63)[489].

Ancora interessante è la sentenza McFadden c. Sony, 15 settembre 2016[490]. Nella fattispecie un negoziante permetteva di utilizzare la propria rete WiFi a chi entrava in negozio e ciò senza protezione o controllo (password). Era capitato che un

[488] Questo passaggio è stato interpretato da App. Milano 07.01.2015 n. 29, Yahoo c. RTI, RG 3821/2011, § 33, nel senso che la tutela d'autore cede di fronte a quella del diritto di impresa (del provider) e del diritto di informazione. Il giudizio non è condivisibile: dire che la tutela di un diritto non è assoluta è solamente l'ovvio presupposto per una conciliazione in cui nessuno astrattamente e in linea di principio viene posposto né anteposto: infatti la stessa affermazione vale per gli altri due diritti antagonisti.

[489] Va segnalata l'opinione dell'AG Villalon, C-314/12, § 78: <<*Un'illecita misura del tipo menzionato sarebbe costituita dall'obbligo imposto dal giudice al fornitore di accesso di ricercare attivamente eventuali copie della pagina illegale sotto altri nomi a dominio o di filtrare tutti i dati trasmessi nella sua rete al fine di stabilire se abbia avuto luogo la trasmissione di specifici film protetti e di bloccare siffatte trasmissioni. Tuttavia non ci sono le condizioni per una siffatta misura nel caso di specie. Il giudice del rinvio deve pronunciarsi, in realtà, sul blocco di uno specifico sito Internet. La misura non viola pertanto l'articolo 15, paragrafo 1, della direttiva 2000/31*>>

[490] C.G. 15.09.2016, *Mc Fadden c. Sony,* C-484/14, quinta, nona e decima questione pregiudiziale, §§ 80 ss.

soggetto appunto nel negozio[491] avesse scaricato materiale illecito: si tratta dunque di uno dei pochi casi giudiziari di semplice trasporto/mere conduit ex art. 12 dir. 2000/31[492]. Nel caso specifico, secondo il giudice a quo, le misure adottabili in concreto erano tre e cioè: i) esaminare tutte le informazioni trasmesse, ii) chiudere la connessione oppure iii) proteggere la tramite password (§ 85). È chiaro che la prima misura contrasta con il divieto di monitoraggio generale e quindi non è ammissibile. Nemmeno è ammissibile la chiusura della connessione, dal momento che compromette troppo la libertà di impresa (§§ 87-88). La Corte ritiene invece che la misura della password obbligatoria sia una misura sopportabile per l'impresa (§ 91) e nemmeno troppo restrittiva per il diritto alla libertà di informazione dei destinatari del servizio (§ 92 e 94). Tale misura è anche sufficientemente efficace[493], sempre che la comunicazione di password agli utenti sia preceduta dalla rivelazione della loro identità per ottenerla e quindi sempre che non possano agire in via anonima (§ 96): il che, però, obbliga il venditore o il titolare della rete locale ad annotare (magari pure a verificare) diligentemente le informazioni personali (il che costituisce trattamento di dati personali[494]).

30. L'inibitoria. Giurisprudenza italiana in tema

C'è pure della giurisprudenza nazionale. Alcune sentenze riprendono quanto stabilito da quelle europee circa l'inammissibilità di un dovere di sorvegliare tutti i file del

[491] Magari anche fuori dal negozio, se la rete WiFi permetteva utilizzi ad una buona distanza.

[492] Il processo era stato promosso con domanda di accertamento negativo dal fornitore del collegamento wifi: § 28.

[493] <<*Devono avere l'effetto di impedire o, almeno, di rendere difficilmente realizzabili le consultazioni non autorizzate dei materiali protetti e di scoraggiare seriamente gli utenti di Internet che ricorrono ai servizi del destinatario di tale ingiunzione dal consultare tali materiali messi a loro disposizione in violazione del suddetto diritto fondamentale*>> (§ 95, richiamando *UPC Telekabel Wien*, C-314/12, § 62).

[494] Per l'AG Szpunar in *Telekabel*, C-484/14, § 132, <<*per costituire un obbligo generale di sorveglianza «in casi specifici» (41), accettabile ai sensi di tale disposizione, infatti, la misura di cui trattasi dev'essere delimitata per quanto concerne l'oggetto e la durata della sorveglianza*>>. L'AG aveva ritenuto non compatibile col diritto UE la misura della protezione della rete wifi (§§ 134-150), opinione non seguita dalla CG.

provider alla ricerca delle opere appartenenti al soggetto leso: così, ad es., il già cit. Appello Milano 07.01.2015 n. 29, Yahoo c. RTI[495] ed pure un reclamo cautelare del Trib. Torino 18.09.2015 in Delta TV c. Dailymotion[496].

In senso opposto v. i giudici di Torino secondo cui "*L'intervento richiesto all'hosting provider, non si sostanzia affatto, come paventano i resistenti, in un vaglio preventivo su tutti i contenuti presenti o in corso di caricamento sulla sua piattaforma, finalizzato a individuare video lesivi dei diritti del ricorrente. Si tratta, invece, di un controllo successivo e mirato. Successivo, perché è stato preceduto da una denuncia in cui sono stati individuati gli specifici URL dei contenuti asseritamente lesivi. Mirato perché è diretto a impedire nuovi caricamenti di quei contenuti che erano presenti agli URL già comunicati. Non convincono le difese di YouTube e Google Inc. nella parte in cui pretendono di individuare i contenuti con gli URL; affermando di conseguenza che ogni nuovo caricamento su un URL diverso rappresenterebbe un "nuovo contenuto" (diverso da quello precedentemente rimosso). E infatti la locuzione Uniform Resource Locator (in acronimo URL), nella terminologia delle telecomunicazioni e dell'informatica è una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa in Internet, tipicamente presente su un host server, come ad esempio un documento, un'immagine, un video, rendendola accessibile ad un client che ne faccia richiesta attraverso l'utilizzo di un web browser. Dunque l'URL non è il contenuto, ma piuttosto il "luogo" dove il contenuto è reperibile. 3.6 Dal punto di vista tecnico, è pacifico che l'attuale stato della tecnologia consente di individuare, fra la sterminata mole di materiale presente su YouTube, quello corrispondente a un determinato contenuto. Questa è la descrizione del funzionamento di Content ID reperibile sul sito di Google: "Content ID è uno strumento sviluppato per consentire ai titolari di copyright di identificare e gestire facilmente il*

[495] App, Milano 07.01.2015 n. 29, *Yahoo c. RTI*, RG 3821/2011, § 61-63 richiama le sentenze della C.G. sopra ricordate..

[496] Non visto ma riportato da Trib. Torino 11.08.2016 ord. sez. feriale, Delta Tv c. Dailymotin, RG 19878/2016, sub § 4, p. 5/6. Questa ord. estiva del 2016 decide un reclamo proposto contro provvedimento cautelare, emesso in sede di opposizione all'esecjuzione (a precetto) ex art. 615 bis cpc (esecuzione a sua volta iniziata in base a provvedimento cautelare reclamato e parzialmente riformato).

copyright dei propri contenuti su YouTube. I video caricati su YouTube vengono esaminati e confrontati con un database di file che abbiamo ricevuto dai proprietari di contenuti. Spetta al titolare del copyright decidere come procedere nel caso in cui i contenuti di un video di YouTube corrispondano a una delle sue opere. In tal caso, il video riceve una rivendicazione di Content ID". Sempre da un punto di vista tecnico, non è vero che questo filtro possa funzionare solo se i reference file vengono forniti dal titolare dei diritti che si assumono violati. L'unica cosa necessaria è che il software disponga di file di confronto, sulla cui base individuare i file simili"[497].

In breve, la tecnologia esistente permette filtraggi automatici, che di conseguenza non costituiscono obblighi generali di sorveglianza o ricerca.

Nello stesso senso Trib. Milano ord. 12.04.2018, Mondadori c. Fastweb, secondo cui <<*tenuto conto delle circostanze del caso concreto, ritiene questo tribunale che sia compatibile con il divieto dell'obbligo generale di sorveglianza, proporzionata e allo stesso tempo efficace una misura che ordini agli internet service provider di impedire l'accesso ai medesimi contenuti già accertati illeciti -perché relativi alle comunicazione al pubblico, senza autorizzazione dell'avente diritto, dei diritti esclusivi della ricorrente relativi ai Periodici*>>[498].

31. (segue:) l'ingiunzione c.d. dinamica

Altri provvedimenti nazionali riguardano la specifica questione dell'ingiunzione cosiddetta dinamica. Si tratta del problema del se si possono inibire pro futuro certe condotte anche se in modalità informaticamente diverse da quello oggetto di causa. Da qui l'aggettivo <dinamiche>, dato che si mira a reprimere l'elusione del provvedimento inibitorio, variando qualche aspetto della condotta contraffattiva: in particolare modificando il server di provenienza tramite i suoi cosiddetti siti alias.

[497] Trib. Torino ord. 23.06.2014, *Delta TV c. Google*, in *AIDA*, 2015-XXIV, *1685*, p. 785 ss, §§ 6.5-6.5; Trib. torino ord. 03.06.2015, *Delta TV c. Dailymotion*, RG 11343/2015, § 8 (e qui sub §§ 3.5-3.6) che riprende pari pari ex 118 c. 1 disp. att. cpc passi della precednte. Descrizione del software di digital fingerprinting *Content-Id*, adottato da Youtube (Google) in Gray J.E., *Google Rules*, cit., 121 ss.

[498] In *Dir. di internet*, 2018/1, 112, sub § 13. nota Molinario. E' la stessa cit. subito dopo sul tema della ingiunzione dinamica.

Secondo Trib. MI 12.4.18[499] si può ordinare ai provider di impedire l'accesso "ai medesimi contenuti già accertati illeciti", a prescindere dal nome di dominio che continua a mutare per dichiarata volontà del violatore. Un diverso comando, che circoscrivesse l'ordine ad un preciso nome di dominio, sarebbe in pratica inutiliter datum. Un ordine dunque che comprenda i siti alias è l'unico che impedisce o rende difficilmente realizzabile l'illecito, secondo lo spunto di C.G. in Telekabel. Il giudice però subordina il sorgere di questo obbligo alla segnalazione da parte del titolare, per evitare di dare contenuto troppo ampio al provvedimento, che potrebbe violare il divieto di monitoraggio generale. L'ordine è ugualmente molto ampio e comprende i contenuti presenti non solo in diversi top level domain (.it,.fr etc.), ma anche con uguale nome di secondo livello[500]: ed anzi pure i contenuti presenti in qualsiasi sito e cioè a prescindere dalla ricorrenza di uguale o diverso nome di dominio di primo o di secondo libello[501]. Ne segue che il soggetto inibito dovrà filtrare a trecentosessanta gradi sui propri server, avendo un solo limite: che si tratti del contenuto dichiarato illecito. Tale dovere è difficilmente compatibile con il divieto di art. 15 § 1 dir. 2000/31-art- 17 c.1 d. lgs. 70/2003.

Nello stesso senso altri due provvedimenti cautelari a cavallo tra il 2019 e il 2020, i quali ammettono l'inibitoria anche relativamente ai siti alias con mutamento non solo del top level domain (fermo il second level domain), ma anche con mutamento di quest'ultimo, <<*a condizione che - oltre a rimandare ai medesimi contenuti illeciti innanzi considerati - il collegamento tra i soggetti responsabili dell'attività illecita ad oggi posta in essere tramite i siti indicati sia obbiettivamente rilevabile; le parti ricorrenti comunicheranno ai resistenti tale estensione sotto la loro responsabilità allegando tutti gli elementi documentali utili ad attestare la provenienza dai medesimi soggetti*>>[502].

[499] Trib. Milano ord. 12.04.2018, *Mondadori c.Fastweb*, in *Dir. di internet*, 2019/1, 107 ss, § 13 e § 20, nota di L. Molinario.

[500] In un ipotetico www.ilmegliodidalla.it, il dominio di secondo livello è ad es. <ilmegliodidalla> all'interno del dominio di primo livello <.it>.

[501] p. 115.

[502] Trib. Milano decr. inaudita altera parte 14.01.2020, RG 601/2020, *Medusa Film e Taodue c. TIM, Vvodafone ed altri*. Negli stessi esatti termini, anche linguistici, uguali parti ed estensore diverso, il di poco precedente Trib. Milano

Proprio su questo punto diverge -andando in senso restrittivo- Tribunale Milano 4 marzo 2019[503], sempre in fase cautelare. Viene infatti parzialmente disattesa l'istanza <<*in relazione al richiesto blocco all'accesso a tutti gli altri siti che in futuro porranno a disposizione del pubblico i medesimi contenuti (i cd. "alias"), posto che l'effettiva riconducibilità ad un unico fatto lesivo dovrebbe essere specificamente vagliata, per verificarne la reale coincidenza oggettiva e soggettiva con i comportamenti già esaminati –dunque effettivamente consistenti nell'attuazione del medesimo comportamento illecito - al di là di quelle condotte che pongono in essere minime variazioni del tutto secondarie e non autonomamente caratterizzanti: allo stato deve dunque estendersi l'inibitoria a quelle condotte che associno diverso top level domain al medesimo second level domain che consiste nell'espressione enigma IPTV, onerando parte ricorrente di comunicare alle resistenti gli eventuali nuovi indirizzi IP che consentissero il collegamento al sito web in questione, anche ove quest'ultimo sia associato a diverso top level domain ma consenta la fruizione dei medesimi contenuti*>>.

Non è esplicitato che questo comportamento del titolare condizioni l'operatività degli ordini inibitori a carico del provider: tuttavia un'interpretazione secondo buon senso induce a ritenere ciò. Il motivo, per cui il tribunale limita l'estensione dell'inibitoria a variazioni di top level domain, è, come visto, che <<l'effettiva riconducibilità ad un unico fatto lesivo deve essere specificamente vagliata>> (da un giudice). Va osservato che,

decr. inaudita altera parte 24.12.2019, RG 62350/2019. Si è fatto notare che i decisori hanno data per scontata la legittimazione passiva dei provider resistenti e che a ragione l'hanno fatto, stante la responsabilità civile degli intermediari disposta dai due safe harbour (europeo e nazionale) e dalla dir. 2004/48 (Cassano G.-Tassone B., *Turbo ingiudnzione dinamica. Il futuro delle tutela delle opere cinamatografiche e non solo, Dir. di internet,* 2020/2, 235). L'affermazione va precisata, se si accetta che il lemma <responsabilità civile> concerne il risarcimento del danno: la legittimazione passiva si basa infatti sull'assoggettabilità al diverso rimedio dell'inibitoria, che prescinde da dolo o colpa. A ben vedere, lo precisano gli stessi giudici milanesi: <<*rispetto a queste violazioni la posizione degli ISP resistenti - astrattamente non responsabili per detti illeciti, ai sensi dell'art. 14, d. lgs n. 70/2003 - assume rilievo in relazione alla loro qualità di intermediari, che consente comunque l'adozione nei loro confronti di ordine inibitorio, a prescindere dalla sussistenza di dolo o colpa per le violazioni prospettate (v. art. 156, comma 1, l.a.)*>>..

[503] Trib. Milano decr. 04.03.2019, in *Dir. di internet,* 2019/1, 106, *Lega Nazionale professionisti Serie A contro Fastweb e altri*, nota di Molinario.

ferma restando l'identità del materiale caricato on line, costituisce sì nuovo fatto, ma processualmente secondario[504], anche il mutamento di dominio di secondo livello e non solo quello di primo livello. In fondo si tratta solo di agganciare gli stessi file e il medesimo server ospitante ad un nome di dominio diverso: è cosa diversa –per fare un paragone col mondo analogico- passare dalla pubblicazione su un periodico a quella su un periodico diverso. Questo non sembra affatto eccedere il concetto di minima variazione secondaria, entro la quale il tribunale afferma di concedere l'ingiunzione dinamica.

Allo stato e a prima vista, dunque, sembra eccessivo ravvisare ad es. una sfera di pubblico diversa e un ampliamento di potenzialità lesiva (e quindi un fatto lesivo diverso) solo per aver cambiato il nome di dominio[505].

Ragiona similmente un provvedimento cautelare del Tribunale di Torino nella lite Delta TV v. Dailymotion, ove pregevolmente analitica motivazione[506].

Secondo il comando ivi portato, la denuncia del soggetto leso con indicazione della url è necessaria solo per la prima violazione, mentre non può essere pretesa per le successive. Per queste ultime può essere dato un'inibitoria ampia, concernente il materiale illecito a prescindere dall'identità totale o parziale della url. Il medesimo contenuto su url diverse, infatti, non è un nuovo contenuto, bensì il medesimo contenuto in un luogo diverso. Del resto, con i sistemi di filtraggio automatizzati tramite opportuni parametri di ricerca, non si viola il divieto di monitoraggio generale: basta infatti impostare i parametri medesimi solamente con il materiale, anzi, meglio, con il file inizialmente accertato come illecito (il Tribunale menziona il sistema dell'impronta digitale –fingerprint- oppure il sistema del

[504] Sulla distinzione tra fatti principali e fatti secondari Comoglio L.P. voce *Allegazione*, in Dig. Civile, Pluris online, 1987. "*§ 5 (...) Data ormai per acquisita la distinzione tra fatti principali e fatti secondari (47), è fuori dubbio che 1'«esclusiva» del soggetto onerato, nei processi di tipo dispositivo, sia limitata all'allegazione dei primi, non impedendo in linea di massima il rilievo e la cognizione ex officio dei secondi, comunque emergenti dalle asserzioni e dal contraddittorio dei litiganti. Nota 47: Gli uni sono direttamente integrativi della fattispecie legale da cui trae origine il diritto azionato od il controdiritto eccepito; gli altri sono fonti conoscitive, per così dire, indirette (o di secondo grado), da cui è dato argomentare l'esistenza, l'inesistenza o il modo d'essere dei primi*".

[505] Si tratta però di opinione provvisoria, che meriterebbe approfondimento.

[506] Ord. 3 giugno 2015, RG 11343/2015.

Content-ID predisposto da Yahoo, in realtà: da Google/Youtube[507] oppure il sistema Ina Signature).

Avrebbe potuto forse essere approfondito maggiormente, data la centralità nell'iter motivatorio e seppur si trattasse di sede cautelare, l'affermazione di <unicità del contenuto> nonostante la provenienza da URL diverse[508]. Sarebbe forse meglio parlare di <unicità del fatto dannoso>, secondo il tenore dell'art. 2043, o di <unicità della violazione>, secondo il tenore degli art. 156 e 158 l. aut. (e dell'art. 124 c.1 cod. propr. ind.).

La successiva sentenza di merito, che ha definito l'opposizione a precetto (notificato per inottemperanza a detta ordinanza cautelare), con un comando assai complesso (alla luce anche della complessità di quello cautelare, anche per la parziale riforma intervenuta in sede di reclamo[509]), ha sostanzialmente confermato la cautela già concessa, così rigettando le istanze del titolare di un ordine di ricerca di materiali già caricati se <corrispondenti> a quelli denunciati[510]. Il motivo di questa differenza non è ben chiaro, dal momento che i filtraggi tecnicamente possibili dovrebbero funzionare allo stesso modo sia in via preventiva che in via successiva sui materiali già

[507] Che oggi gli affianca altro software chiamato *Copyright Match Tool*: v. le informazioni fornite dalla stessa società. Content-ID dà al titolare la scelta se bloccare o permettere ma in tale caso incassando una parte del corrispettivo per la pubbblicità agganciata al file de quo o infine permettere ma senza agganciamento ad alcuna pubblicità (*block, monetize or track*): Geddes K., *Meet Your New Overlords: How Digital Platforms Develop and Sustain Technofeudalism*, cit., 461/2; DeLisa N.T., *You(Tube), Me, and Content ID: Paving the Way for Compulsory Synchronization Licensing on User-Generated Content Platforms*, cit., pp. 1280-1284; Gray J.E., *Google rules,* cit., 121 ss. Geddes evidenzia che questo sistema sfrutta il lavoro altrui (cioè dei violatori) in contrasto con la disciplina del Copyright Act, che mira a bilanciare la deterrenza contro la violazione con l'incentivo alla creatività (Id., op. cit., 476 ss., che scrive di *unjust enrichment*): il tema è complesso, anche perché tale facoltà sarà stata accettata contrattualmente, sicchè bisognerebbe ragionare sulla validità della relativa clausola. Microsoft ha sviluppato *Photo-DNA* per il filtraggio delle fotografie (Bloch-Wehba H., *Access to algorithms*, 20).

[508] Il che avrebbe richiesto di chiarire il concetto informatico di URL: v. ad es. la relativa voce in Wikipedia.

[509] in breve la cautela, a seguito del reclamo, impartiva un complesso comando, sulla base di una duplice distinzione: da un lato, tra caricamenti già avvenuti e caricamenti futuri e, dall'altro, tra i medesimi contenuti già denunciati tramite url e contenuti ad essi <corrispondenti>-

[510] Trib.Torino 24.1.2018, *Dailymotin v. Delta TV Programs*, RG 5135/2015, pagg. 26-27.

presenti nei server del provider.

32. Sintesi sul divieto di istituire un obbligo generale di sorveglianza o ricerca ex art. 17 c. 1. Il caso europeo *Eva Glawischnig-Piesczek c. Facebook Ireland limited,* C-18/18

Il contenuto del divieto di monitoraggio generale, dunque, è di difficile determinazione, stante la vaghezza delle relative disposizioni: come osservato sopra, sono possibili le opposte interpretazioni. Potrebbe avere infatti qualche ragione pure la tesi, secondo cui l'obbligo generale non viene intaccato, quando l'ordine riguarda uno specifico file o anche una specifica opera protetta, a prescindere dal server tramite il quale viene messa on-line: quindi nemmeno quando il file va intercettato su tutte le possibili fonti di provenienza. Si tratta sempre di un obbligo di ricerca specifico, che non può essere ritenuto violazione del divieto di sorveglianza e ricerca generali. L'impressione, però, è che questa interpretazione estensiva troverà peggior accoglienza di quella che può considerarsi il suo opposto (dovere di ricerca di un certo file/opera protetta su certe fonti/server). Il problema è semmai più complesso quando la violazione è ridotta e cioè nel caso di diritto d'autore comporti una riproduzione solo parziale oppure quando il diritto leso e quello all'onore e alla reputazione. In quest'ultimo caso, infatti, si pone il problema del se le condotte successive alla diffamazione iniziale costituiscano ripetizione del medesimo illecito ed anzi se costituiscono ancora illecito (e eventualmente il medesimo illecito).

Su quest'ultimo problema (che si candida ad essere uno dei più difficili da dipanare) fa un po' di luce il caso europeo Eva Glawischnig-Piesczek c. Facebook Ireland Limited, C-18/18. Secondo la C.G.[511] sono compatibili col diritto UE le ingiunzioni ad un host provider di rimuovere le informazioni di contenuto identico (si badi: identico) a quello dell'informazione già dichiarata illecita o di bloccarne l'accesso, chiunque sia l'autore dell'uploading (cioè sia l'autore già parte del processo, sia soggetti terzi)[512]. Ed è compatibile pure fare altrettanto (v. però

[511] C.G. 03.10.2019, C-18/18, § 37.

[512] Concorda su questga interpretazione, che differenzia così significativamente la sentenza dalle conclusioni dell'AG, Monti M., La Corte di giustizia, la direttiva e-commerce, cit., , § 3. Secondo Keller D., *Dolphins in the Net: Internet Content Filters and the Advocate General's Glawischnig-Piesczek*

la precisazione subito sotto per il profilo soggettivo) circa l'informazione di contenuto non identico, bensì solamente equivalente (si badi: equivalente, non più identico) a quello già dichiarato illecito (§ 41 ss). Circa le informazioni equivalenti, però, punctum dolens di questo tipo di liti, la Corte precisa che non può esserci un obbligo eccessivo imposto al provider: devono allora essere specificate debitamente gli elementi dell'ingiunzione, come il nome della persona interessata, le circostanze e il contenuto equivalente. Comunque <<*differenze nella formulazione di tale contenuto equivalente rispetto al contenuto dichiarato illecito non devono, ad ogni modo, essere tali da costringere il prestatore di servizi di hosting interessato ad effettuare una valutazione autonoma di tale contenuto*>> (§ 45), sicchè quest'ultimo può avvalersi di tecniche e mezzi di ricerca automatizzati (§ 46)[513]. Ad essere precisi, però, e circa le informazioni <equivalenti>, la C.G. non dice espressamente che c'è l'obbligo di filtrarle verso qualunque utente: semplicemente tace su questo profilo soggettivo[514], a differenza dalla presa di

v. Facebook Ireland Opinion, 04.09.2019, Center for Internet and Society at Stanford Law School, 30, l'affermata possibilità di filtrare tutti i contenuti identici da chiunque provenienti contrasterebbe con la sentenza C.G. in *L'Oreal c. eBay* del 12.07.2011, C-324/09, § 139. Tuttavia non pare sia così. E' vero che in tale § 139 si legge <<*the measures required … cannot consist in an active monitoring of all the data of each of its customers*>>, come riporta l'a.: il che porterebbe ad ammettere detto contrasto. L'a. però omette di riportare il prosieguo (<<*in order to prevent any future infringement of intellectual property rights via that provider's website*>>): dal quale si desume che il divieto di monitoraggio generale è violato se l'inibitoria riguarda tutti i dati di tutti i clienti per qualunque violazione di diritti IP. *Dictum*, allora, che non contrasta con un ingiunzione di filtraggio per qualunque cliente, ma solo per gli specifici (identici) fatti di causa.

[513] Secondo un a., la necessità che l'ingiunzione si limiti ai filtraggi automatici deriva dal fatto che, secondo l'AG, l'impiego invece di *human review* farebbe perdere il safe harbour ex art. 14 (Keller D., *Dolphins in the Net*, cit., p. 31/33, con rifereimento al § 61 delle Conclusioni). Ma non pare sia così: la preoccupazione del'AG è invece quella di non gravare di costi eccessivi i provider, come emerge chiaramente dall'analogo passaggio della sentenza della C.G. (§ 45 riferito al § 44 <<*l'obiettivo perseguito da un'ingiunzione …. non può essere perseguito mediante un obbligo eccessivo imposto al prestatore di servizi di hosting*>>). Ad ogni modo è certo che evitare ogni *human review* incrementi di molto il tasso di errori, ledendo diritti fondamentali come quello di libertà di parola, di critica e/o di fair use in genere (Keller D., *Dolphins in the Net*, passim, ad es. p. 17/8, 26).

[514] Letti e riletti i §§ 38-47, mi pare che ricorra il silenzio indicato nel testo. Se così è, diventa allora troppo frettoloso affermare invece che la C.G. abbia ammesso il filtraggio di cotnenutoi eqjuivalenti verso tutti (così Keller D.,

posizione specifica dell'AG, che ne aveva ammesso il filtraggio solo verso il medesimo utente (v. subito sotto). Viene il sospetto che nella fretta (la decisione corre infatti un po' troppo spedita)[515] il relatore si sia dimenticato di questo profilo soggettivo, non potendosi pensare ad un consapevole silenzio su un punto così importante.

Le relative conclusioni dell'avvocato generale Szpunar[516] erano più analitiche e in particolare differivano dalla sentenza sul punto della inibitoria di informazioni non identiche, bensì solo equivalenti. L'AG infatti aveva ritenuto ammissibili queste ultime (le "equivalenti") solo se a carico del medesimo utente

Facebook Filters, Fundamental Rights, and the CJEU's Glawischnig-Piesczek Ruling, in *GRUR International*, Volume 69/6, June 2020, 620).

[515] La C.G. non ha per nulla raccolto l'invito a curare i dettagli dell'importante caso sottopostole, avanzato dalla dottrina specialistica all'indomani delle conclusioni dell'AG (ad es. da Keller D., *Dolphins in the Net*, cit., passim). Keller rileva insoddisfacenti genericità già nelle Conclusioni del'AG (passim, ad es. p. 4, 18/9, 22). L'a. astrattamente ha certo ragione: solo che processualmente la cosa è complicata, poiché, da un lato, il giudice europeo è vincolato dal tenore delle questioni pregiudiziali e, dall'altro, la risposta della C.G. prescinde dall'applicazione ai fatti di causa (spettante solo al giudice a quo). Sarebbe stato dunque problematico, in presenza di questioni pregiudiziali astratte, immaginare (forse meglio: divinare, data la rapidità dei mutamenti tecnologici) scenari concreti, esaminando ipotesi e sottoipotesi informatiche (quindi con consuolenza tencica), per dare a ciascuna di queste una risposta specifica. E' interessante poi l'osservazione per cui nel processo europeo sono state sentite solo le parti dirette (oltre ai Governi) e non altri stakeholders della società civile (op. loc. ult. cit., p. 7/8; e in Keller D., *Facebook Filters, Fundamental Rights, and the CJEU's Glawischnig-Piesczek Ruling*, cit., p. 623). Né la Corte ha accolto (nel senso che non vi fa alcun riferimento) l'invito dell'AG ad occuparsi del limite temporale al dovere di monitoraggio (§ 49, invocando i §§ 45-46 di C.G. 16 febbraio 2012, *Sabam c. Netlog*, C-360/10): così giustamente De Gregorio G., *Moderazione dei contenuti in rete. Poteri privati tra prospettive locali e prosettive globali*, in *Quaderni costituzionali*, 2020/1, p. 178. Secondo un a., la sentenza *Glawischnig-Piesczek* non ammette l'inibitoria verso chiunque e per contenuti non identici ma solo simili: questi ultimi potranno essere bloccati *erga omnes* solo dopo notificazione *ad hoc* (o specifica menzione in sentenza; ma allora non è più dinamica!): infatti, delle due variabili dinamiche (infringer/contenuto; e cioè profilo soggettivo ed oggettivo della violazione), almeno una delle due non può restare indeterminata (van der Donk B.B.E., *How dynamic is a dynamic injunction? An analysis of the characteristics and the permissible scope of dynamic injunctions under European Law after CJEU C-18/18 (Glawischnig-Piesczek)*, in *Journal of Intellectual Property Law & Practice*, Vol. 15/8. 2020, p. 608/611 (ove utile esame dei termiin della questione).

[516] Conclusioni AG Szpunar 04.06.2019, C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*; C.G. 03.10.2019, C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*.

già coinvolto giudiziariamente: le aveva invece ritenute non ammissibili se a carico di terzi. Qui però il motivo non è molto chiaro, poiché il dire che ciò richiederebbe la sorveglianza della totalità delle informazioni diffuse sulla piattaforma (§ 73) non sembra giustificato: l'AG pone l'accento sulla necessità di soluzioni tecnicamente sofisticate, quando si tratta di individuare informazioni equivalenti anziché quelle identiche, e sul fatto che dovrebbe esercitare una forma di censura, diventando quindi un contributo reattivo e non più solo passivo della piattaforma (§ 73). Tuttavia sono osservazioni di dubbia persuasività, dal momento che, se dette soluzioni tecnicamente sofisticate sono automatiche, non dovrebbe esserci differenza a seconda che siano calibrate su uno, due, tre o su tutti gli utenti.

Il vero problema, piuttosto, oltre a quello della individuazione della equivalenza, sarà quello di decidere (toccherà al giudice, difficilmente interverrà il legislatore)[517] quale sia il livello di investimento tecnologico richiesto ex diligentia (oppure ex non culpa, se in via aquiliana). C'è da decidere se pretendere l'adozione dei migliori software da tutti i provider indistintamente oppure se calibrare la pretesa in base alle dimensioni (cioè essenzialmente, in base al traffico, direi) di ciascuno. Pare esatta la seconda alternativa: da un lato, perché così induce a pensare l'applicazione della diligenza o della non colpa; dall'altro perché non si può pretendere che anche i provider minori adottino i software più avanzati, pochi e costosi, pena la loro espulsione dal mercato, con la conseguenza di lasciare quest'ultimo in mano a pochi colossi mondiali tecnologici. Considerazione concorrenziale, che certo rileva in sede di interpretazione delle norme civilistiche, la quale, a parità di altri fattori, deve essere "orientata alle conseguenze" della propria applicazione[518]. Una conferma può trovarsi nella recente

[517] Però l'ha fatto quelo europeo in tema di copyright (dir. 790/2019), come dirò tra un attimo.

[518] E' disponibile un report molto interessante relativo ad un sondaggio condotto tra provider statunitensi circa l'applicazione della procedura di *notice and take down* ex § 512 DMCA (esamina pure alcune specifiche procedure di notice and take down): Urban J.-Karaganis J.-Schofield B.L., *Notice and Takedown in Everyday Practice* (March 22, 2017), *UC Berkeley Public Law Research Paper No. 2755628*, leggibile in *ssrn.com*. In base al grado di automazione nel gestire le procedure, gli aa. dividono i provider in tre categorie, che loro –in ordine di crescente capacità finanziario- tecnologiche, chiamano *DMCA Classic*, *DMCA Auto* e *DMCA Plus*. Ebbene, si legge che i provider minori

modifica del copyright europeo, che, seppur in termini non chiarissimi, dovrebbe permettere la calibratura accennata[519].

Come già accennato sopra, le condizioni e le modalità dell'inibitoria sono regolate dal diritto nazionale, non europeo, purchè non contrastino con norme europee: e dunque, circa gli internet provider, non contrastino con la dir. 2000/31[520] né con la dir. 2004/48 (ed oggi nemmeno con la dir. 2019/790). Il tema della ampiezza del contenuto inibito affinchè, sufficientemente esteso da non essere aggirabile ma non troppo da essere penalizzante per la libertà di azione dell'ingiunto o da diventare una mera ripetuizione della norma di legge, è stato esaminato dalla dottrina sia industrialistica che processualistica. Il problema, naturalmente, è capire quando la condotta successiva rientri in quella già inibita (costituendo quindi violazione dell'inibitoria stessa), senza dover proporre una nuova e autonoma azione di accertamento: ma i profili sono connessi, dal momento che più ampia è l'inibitoria, più facile sarà farvi rientrare la condotta successiva. Quando invece l'inibitoria ha un contenuto assai ristretto, c'è il rischio che in pratica si limiti ad inibire solo comportamenti uguali a quelli accertati illeciti. Secondo una dottrina i limiti oggettivi del giudicato, sottostante all'inibitoria, sono rispettati se i due comportamenti messi a paragone (quello accertato illecito e il successivo) sono accomunati da identità di genere e di specie, all'interno della quale eventuali diversità fenomeniche non escludono l'operatività del provvedimento[521]. Stante però la genericità di

(DMCA Classic) sono assai preoccupati che l'imposizione dei filtri più avanzati comporti pesanti vantaggi per i concorrenti di maggior dimensione; si legge pure che di ciò si curano poco i titolari di diritti (sarebbe strano l'opposto!): v. ivi, sub E, pp. 64-67. L'indagine è esposta più concisamente dagli stessi aa. in due saggi successivi: *Notice and Takedown: Online Service Provider and Rightsholder Accounts of Everyday Practice* (November 1, 2017). 64 J. *Copyright Soc'y 371*, Summer 2017, leggibile in *ssrn.com* e *Takedown in Two Worlds: An Empirical Analysis* (February 1, 2018), 64 J. Copyright Soc'y 483, pure leggibile in *ssrn.com*.

[519] Art. 17 dir. UE 2019/790, §§ 4-6.

[520] Conclusioni 04.06.2019 AG Szpunar, C-18/18, Eva Glawischnig-Piesczek c. Facebook, § 33.

[521] Ghidini G., *Della concorrenza sleale. Artt. 2598-2601*, in *Il cod. civ. comm.* dir. da Schlesinger, 1991, 394-395. Che il giudice debba indicare il genere dell'atto inibito, lo scrive pure Libertini M., *Azioni e sanzioni nella disciplina della concorrenza sleale*, in Ghidini G.-Libertini M.-Volpe Putzolu G., *La concorrenza e i consorzi* in *Tratt. dir. comm. e dir. pubbl. ecn.* dir. da Galgano, CEdam, 1981, 245/6.

questo primo criterio, l'autore lo precisa affermando l'irrilevanza del fattore tempo e del fattore luogo nonché di altre modalità di compimento, che ai fini degli effetti lesivi sono equivalenti. Per certi tipi di illeciti ciò può risultare di più facile applicazione. ad es. quando si tratti di violazione di marchio o di diritto d'autore o di brevetti rispetto alle diffamazioni[522]. In tali casi si potrà ricorrere al concetto di <<nucleo della violazione concreta>>, elaborato dagli ambienti giuridici tedeschi e svizzeri: il quale non si allontana molto da quello appena visto di "specie e genere"[523] ma può essere utile, perché comporta un richiamo ai criteri propri della privativa industrialistica per ravvisare o meno il ricorrere della identità di violazione. Si pone allora il problema del se questa individuazione del <nucleo della violazione> debba essere lasciato all'eventuale contestazione dell'inibito (oggi verosimilmente contestazione alla penalità di mora ex art.614 bis) o se possa ex ante essere in qualche modo precisato dal giudice. Con la conseguenza in tale caso di dover capire se la precisazione sia vincolante (se cioè, al di fuori di essa, si tratta sempre di violazione diversa da quella accertata illecita) o se possa a sua volta essere intesa con una certa larghezza o elasticità o comunque interpretata: questione che a sua volta trova risposta diversa a seconda che l'ambito, che il giudice

[522] Proprio questo evidenziano le cit. Conclusioni AG Szpunar 04.06.2019, C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, § 71.

[523] Approfonditamente Spolidoro M.S., *Le misure di prevenzione nel diritto industriale*, Giuffrè, 1982, p. 84 ss.. Questo a. ha sostenuto la nota tesi, per cui l'inibitoria non si differenzia dall'accertamento dell'illecito: ivi, p. 41-81., passim Ma a parte che la distinzione è talora presente nei testi di legge (il che è il meno, dato che non impedirebbe una diversa ricostruzione dogmatica, purchè non *abrogans*), l'accertamento mero non può essere titolo esecutivo. Serve in tale senso una condanna ad un facere (per doveri in positivo) o un'inibitoria (per doveri di astensione): così Cass. 10.07.2019, n. 18572, che richiede una condanna almeno implicita (si trattava di un fare infungibile: iscrizione di un lavoretore in certi elenchi dell'INPS). Nel senso della tesi di Spolidoro –almeno a livello pratico; a livello teorico è da vedere- sono due sentenze del Tribunale Torino secondo cui, stante la facilità di filtraggio una volta notiziato dell'illeciti tramite url (e in assenza di seria rivendicazione dall'uploader), il provider automaticamente deve impedire futuri caricamenti in base al dovere di collaborazione emergente dall'art. 16 d. lgs. 70/2003 e dai <<canoni di diligenza cooperazione e buona fede ex art. 1173, 1375 e 1176>> (la seconda richiamata imporopriametne dato che manca un contratto tra provider e soggetto leso): Trib. Torino sent. 1928 del 07.04.2017, RG 38112/2013, *Delta TV c Google – Youtube*, cit., p. 37/8; Trib. TO 24.01.2018, RG 5135/2015, *Daily motion c. Delta TV*, pp. 20-21.

afferma coperto dalla inibitoria, sia indicato in modo più o meno preciso e a seconda che ricorra o meno una statuizione esplicita per chiarire proprio la questione di tale vincolatività. E' stato suggerito che siano le parti (in sede di domanda) e il giudice (in sede di sentenza) a precisare le condotte, rientranti ad es. nel concetto di "ogni violazione o inosservanza successivamente contestata" di cui all'art. 124 c.2 c.p.i, nel giusto mezzo tra dettaglio e ampiezza[524].

La dottrina processualistica ha altresì condivisibilmente posto l'accento sulla necessità che il giudice fissi un limite temporale di operatività della misura coercitiva, non potendosi immaginare nemmeno in astratto un'astrainte perpetua. Con la conseguenza che, decorso il periodo di tempo indicato, si prenderà atto della inutilità dell'astreinte e al creditore residuerà solo la tutela risarcitoria per equivalente ed eventualmente quella in forma specifica[525].

[524] Vanzetti M., *Contributo allo studio delle misure correttive e delle sanzioni civili nel diritto industriale: i profili processuali della articolo 124 c.p.i.,* in *Riv. dir. ind*., 2010 I, 45 e 52/ 53; Spolidoro M.S., *Profili processuali del Codice della proprietà industriale*, in *Il diritto industria*le, 2008/2, 182-183, che evidenzia la difficile applicabilità del concetto di <giusto mezzo>.

[525] Consolo C., *sub art. 614 bis, Cod di procedura civile. Comm.* dir. da Consolo, t. III, sesta edizione, 2018, sub viii, p. 39. Secondo questo a. (in *Spiegazioni di diritto processuale civile, I) Le tutele (di merito, sommarie ed esecutive) e il rapporto giuridico processuale*, Giappichelli, 12 ed., 2019, 80-81), l'inibitoria: i) ha una efficacia determinativa dell'obbligo generico violato; e ii) la sua violazione comporta una responsabilità risarcitoria potenziata, nel senso (pare) di una liquidazione di maggior ammontare per la natura particolarmetne rea della violazione. A questo proposito, osserverei: - sub i) che la determiazione sta più nell'accertamento a monte di illiceita della condotta sub iudice, che nell'inibitoria: la quale, se non è di mera cessazione, si limita a proibire lo stesso comportamento (se in atto) o lo stesso tipo di comportamento (qualora ci sia il rischio di ripetizione). Avrà invece natura determinativa quando manchi l'accertamento a monte e sia totalmente preventiva, quando cioè non ci sia ancora la consumazione di un illecito ma solo il pericolo di esso: eventualità tutelabile non solo in via cautelare ma anche nel merito appunto con l'inibitoria (diversi aa. tra cui Frignani A., *L'injunction nella common law e l'inibitoria nel diritto italiano*, Milano, 1974, 430; contrario Nardo G.N., *Profili sistemtici dell'azine civile inibitoria*, cit., 90-91, per il quale i casi espressi costituscono eccezione; sorprendentemente ritiene, che il "timore di una [futura] violazione" ex art. 156 l. aut. costituisca già un illecito, Basilico G., *La tutela civile preventiva*, Milano, 2013, 251), la quale costituirà provvedimento in futuro, non di condanna ma accertativo-costitutivo; - circa sub ii), poi, osserverei che un risarcimento del danno potenziato costituisce una sanzione, non compensazione, per la parte eccedente il danno allegato e provato: la quale è possibile solo nei casi espressamente previsti dalla legge, che però nulla pare prevedere in proposito per

33. L'art. 17 c. 2

L'articolo 17 c.2 pone due obblighi a carico del provider: 1) informare senza indugio l'Autorita', quando sia a conoscenza di presunte attività o informazioni illecite. Qui è probabile che non ci sarà molto contenzioso, dal momento che il provider, ogni volta che abbia conoscenza di ciò (in pratica, quando venga avvisato dal titolare del diritto asseritamente violato), invierà rapidamente una comunicazione alle Autorità competenti. Farà lo stesso -non è difficile ipotizzarlo- quando ne verrà a conoscenza in qualunque altro modo: non ci sono grossi interessi contrari a ciò (parrebbe). 2) obbligo di fornire a richiesta dell'autorità le informazioni in suo possesso che permettono di identificare il destinatario dei servizi suo cliente. E' stato sollevato il dubbio se da questa norma si desuma un obbligo di identificare il cliente stesso (e magari identificarlo con un certo rigore, cioè senza limitarsi a prendere per buone le dichiarazioni in sede di stipula contrattuale). La risposta è nel senso che, quantomeno in base a questa norma, non c'è obbligo in tal senso. Il dettato normativo è abbastanza chiaro nel dire che l'obbligo di comunicazione riguarda le sole informazioni, che siano in possesso del provider e cioè che siano già (attualmente) in suo possesso: dalla disposizione non si desume che gli a monte abbia specifici doveri di raccolta di questo o quel dato e/o di verificarli. In altre parole, la norma si riferisce alla comunicazione di dati identificativi, di cui sia già in possesso, secondo la sua impostazione di business, mentre non si può da essa trarre che abbia un obbligo di procurarseli[526].

---

la violazione dell'inibitoria (altra cosa è l'astrente ex art. 614 bis). La pravità (o maggior pravità) rileverà in sede punitiva (v. art. 11 L. 689 /1981 sulle sanzioni amministrative; art. 133 c. pen.), non in sede risarcitorio-compensativa (tema amplissimo: v. ora cenni comparatistici in Tichy L., *Preventive liability and system of sanctions in tort law*, in Hofmann F.-Kurz F. (eds.), *Law of remedies*, cit., § 6, pp. 181-185). Per cui la rilevanza delle pravità, quando prevista, perderà tale sua natura: si v. ora nella responsabilità medica l'art. 7 L. Gelli bianco 8.03.2017 n. 24, c. 3, ove il giudice può modulare il risarcimento del danno – patrimoniale, parrebbe- a seconda del rispetto delle linee-guida o delle buone pratiche clinico-assistenziali, per cui alla funzione compenstiva si aggiungerà quella punitiva o premiale a seconda che il quantum sia aumentato o diminuito (entrambe le possibilità parrebbero ammissibili).

[526] I servizi di *identity verification* sono tra i probabili sviluppi di business dei social e in particolare di Facebook: v. Haan S.C., *Bad actors: authenticity, inauthenticity, speech, and capitalism*, cit., passim. ad es. p. 636 e p. 666. L'a.

E' stata affermata l'opposta soluzione, in base alla regola di diligenza professionale, da interpretare alla luce del precetto costituzionale di solidarietà, anche per la gravità dei danni possibili[527]. L'argomento non persuade: ogni prestazione deve essere prevista per legge ex art. 23 Cost., dato che ad essa si contrappone la libertà dei singoli e -per l'imprenditore- la libertà di impresa. Eventuali doveri –magari astrattamente auspicabili- non possono essere tratti dalla fantasia o dalla personale visione dell'interprete, ma solo da volontà legislativa espressa: la quale è troppo evanescente nel caso dell'art. 17 del d. lgs. 70/2003 per arrivare ad una simile conclusione.

Nella pratica, alcune informazioni identificative il provider le avrà sempre[528], dato che avrà stipulato un contratto col proprio utente. Per cui il problema si sposta su un eventuale obbligo di verificare la veridicità dei dati stessi (che ha o che dovesse -in base alle testé respinta tesi- procurarsi): e la risposta è anche qui negativa, non potendosi trarre un obbligo di simile controllo né dall'art. 17 né dal riferimento alla diligenza del cons. 48[529].

Si tratta insomma di regola pubblicistica tra provider e Autorità, nella quale non pare pertinente un richiamo alla diligenza di comportamento, che caratterizza invece i rapporti tra privati, contrattuali o aquiliani che siano. Per non dire, poi, che: i) il riferimento alla diligenza non sta nell'articolato ma solo nel cons. 47; ii) non è imposta ma è lasciata impregiudicata – cioè è dichiarata compatibile col diritto UE- qualora gli Stati intendano imporla; iii) il cons. 47 richiede che sia prevista dal diritto nazionale, il che non è avvenuto da noi.

Non pertinente, poi, è appoggiare la tesi all'inciso <che

affronta in dettaglio il tema della *identification/authenticity*, cui Facebook attribuisce importanza centrale (<*Facebook's authenticity regulation is the substrate upon which its business model is built*>, p. 636), naturalmente per motivi pure di business, oltre che per quelli dichiarati del miglioramento del dibattito sulla sua piattaforma (parte I, p. 631/2 e parte II, passim, ad es. 629-630, 635/6, 640/1 e 665 ss), al punto che il controllo sulle identità supera quello sui contenuti (ivi, p. 643).

[527] Di Ciommo F., *Evoluzione tecnologica e regole di responsabilità civile*, ESI, 2003, 343-345, criticato da Manna 219.

[528] E le conserverà, altrimenti non potendo agire a tutela delle proprie ragioni qualora ce ne fosse necessità.

[529] Conf. Manna L., *La disciplina del commercio elettronico*, cit., pp. 214-215, ove indicazione di tesi contrarie.

consentano l'identificazione>, presente nell'art. 17 c.2 sub b)[530]: la disposizione significa solo che, tra le informazioni in suo possesso, il provider deve comunicare tutte quelle utili per raggiungere l'identificazione. La costruzione sintattica è chiara in tale senso.

La sanzione per la violazione di tali obblighi potrà essere sia penale (favoreggiamento personale, se non concorso nel reato), sia civile (risarcimento del danno ex artt. 2043-2055[531]), ricorrendone i presupposti. Se infatti tale omissione cagiona o contribuisce a cagionare danno (prova difficile), questo sarà ingiusto e del resto sussisterà almeno la colpa: sicchè la risarcibilità difficilmente potrà essere evitata[532].

34. L'art. 17 c. 3. Cambiamenti in vista per la disciplina del safe harbour (ed anzi, delle piattaforme in generale)?

Il c. 3 dell'art. 17 non ha una chiara portata. Afferma la responsabilità civile del provider per il "contenuto di tali servizi" (cioè quelli propri dei tre tipi di provider: artt. 14-16)[533]in due casi: i) quando, richiesto dall'autorità, non ha agito prontamente per impedire l'accesso ai contenuti stessi; ii) quando, pur sapendo della illiceità o dannosità del contenuto da lui ospitato,

[530] Di Ciommo F., *Evoluzione tecnologica e regole di responsabilità civile*, cit., pp. 346-347.

[531] Di Ciommo F., *Evoluzione tecnologica*, cit., p. 344 testo e nota 214, per il quale si tratterebbe di danno distinto da quello prodotto dall'utente uploader e quindi pure di responsabilità del provider distinta da quella dell'utente stesso. Il che non è, poiché il danno, derivante da mancata collaborazione o infomazione circa l'uploader di materiali illeciti, è appunto quello derivante dal- (protrarsi del-) la pubblica esposizione dei materiali medesimi.

[532] Contrario Pino G., *Assenza di un obbligo generale di sorveglianza a carico degli internet service providers sui contenuti immessi da terzi in rete*, in *Danno e resp.*, 2004, 836. che rileva la diferenza dal c. 3: secondo l'a. tali doveri erano già presenti nel ns. ordinamnento in base a norme del c.p.c., come l'art. 118, 210, o del c.p.p. come gli artt. 194, 244 351 e 362. L'affermazione è di dubbia esattezza, almeno con riferimento alle disposizioni del c.p.c.. Ad es. circa l'art. 210 cpc, è assai dubbio che l'informazione identificativa di un cliente del provider possa costituire <<documento o cosa di necessaria acquisizione al processo>> contro il provider medesimo: servono semmai ad ampliare il novero dei soggetti contro cui agire, non certo a decidere la lite pendente contro il provider. Comunque queste disposizioni presuppongono un processo pendente, mentre l'art. 17 c. 2 è applicabile anche al di fuori di esso.

[533] "Responsabile del contenuto di tali servizi" pare da riferire a "nella prestazione dei servizi di cui agli articoli 14, 15 e 16", presente nel c.1 del medesimo art. 17.

non ha informato l'Autorità competente. Si tratta di due fattispecie, in cui la responsabilità è affermata in positivo, anziché in negativo (cioè disciplinandone l'esenzione), come invece avviene negli artt. 14-16. Il che conferma la difficoltà della tesi, che interpreta in positivo pure i predetti artt.14-16, come taluno pur sostiene (anche se la differenza alla fine potrebbe risultare modesta, come sopra accennato)[534].

Circa il caso sub i), "prontamente" vale "immediatamente", di cui all'art. 16 lett. b): non vedo differenza. Si richiede l'impedimento dell'accesso (disabilitazione o filtraggio: da vedere sotto il profilo tecnologico quali modalità esistano), ma non si dice nulla sulla rimozione: e se l'Autorità ordina quest'ultima, invece della disabilitazione? La norma pare riferire la richiesta solo alla disabilitazione all'accesso, ma non impedisce –direi- che venga chiesta invece la rimozione. In tale caso (rimozione) l'inottemperanza può generare danno ingiusto risarcibile? Direi di si. Anche se la colpa non sarebbe per "inosservanza di ordini" (art. 43 c.p.), ma per negligenza generale: dunque sarebbe da invocare ai fini della causa petendi la violazione dell'art. 2043, anziché la norma de qua[535].

La disposizione pare sanzionare con responsabilità civile la stessa condotta che, all'opposto e cioè in negativo, costituisce l'esenzione di cui all'art. 16 c. 1 lett. b), pur se con alcune modeste differenze. Quest'ultima disposizione: i) parla di "comunicazione", anziché di "richiesta"; ii) parla di rimozione/disabilitazione, mentre quella ora in esame, come detto, menziona solo l'impedimento dell'accesso[536]; iii) parla di "autorità competenti", mentre la prima di "autorità giudiziaria o amministrativa avente funzione di vigilanza"; iv) usa l'avverbio "prontamente", invece di "immediatamente". Non sorgono però

[534] Bocchini infatti dice sì che gli artt. 14-16 non sono solo un safe harbour ma una disciplina positiva della responsabilità: sostanzialmente perché, se il provider viola tali norme, sarà assai difficile che riesca per altra via ad andare esente da responsabilità.

[535] La disposizone de qua, espressamente riferita all'impedimento dell'accesso, potrebbe anche ritenersi non eccezionale, all'interno della disciplina del safe harbour, e dunque suscettibile di estensione analogica al caso della richeista di rimozione. Tuttavia l'art. 23 Cost. cit. costituirebbe un serio ostacolo in tale senso.

[536] Inoltre usa il termine *impedire* l'accesso, mentre l'art. 16 c. 1 quello di *disabilitare* l'accesso: non dovrebbe esserci differenza, dato che entrambi si riferiscono al rendere impossibile a terzi l'accesso ai materiali illeciti in contestazione.

particolari problemi interpretativi per le prime due differenze[537], dato che anche dette ipotesi, ammesso che fuoriescano dal safe harbour (art. 16), saranno governate dalla generale clausola di colpevolezza (aquiliana o contrattuale). Il che ad es. significa –circa la differenza sub i)- che, se per caso (ipotesi teorica) l'Autorità si limitasse a "comunicare l'illecito" invece che "richiedere l'impedimento dell'accesso", il provider dovrebbe probabilmente provvedere lo stesso, a pena di (perdere il safe harbour e) rispondere per negligente omissione.

In breve, la disposizione parrebbe inutile, dato che, anche senza di essa, non ci sarebbe dubbio che l'eventuale danno cagionato dall'omissione, ivi regolata[538], sarebbe ingiusto e cagionato con colpa: ovvero, se si opta per la qualifica contrattuale, che sarebbe stato prodotto da inadempimento consistente in condotta negligente.

Inoltre, se si concorda sul giudizio di incostituzionalità della regola (secondo cui è solo violando la comunicazione dell'Autorità che si perde il safe harbour e della –conseguente- possibilità invece di conservarlo nonostante una richiesta (o notizia) di rimozione/disabilitazione avanzata da privati, come sopra osservato circa l'art. 16 § 1 lett. b), l'incostituzionalità si estenderà probabilmente pure alla disposizione in esame. Appare incongruo, infatti, che la perdita del safe harbour venga legata alla notitia criminis anche privata, mentre il risarcimento del danno rimanga legato all'ordine dell'Autorità. Tra il primo momento (notitia criminis privata) e il secondo (comunicazione dell'Autorità), la permanenza on line dei file illeciti sarebbe giuridicamente in una terra di confine, con qualificazione giuridica spuria: priva di safe harbour (per la caduta della disposizione attuale a causa della sua incostituzionalità), ma non soggetta a risarcimento del danno. La logica di questa disciplina sfuggirebbe, non vedendosi interessi da soddisfare suo tramite: per cui non resta che concludere nel senso che anche la disposizione in esame sarebbe incostituzionale.

Il legislatore europeo, del resto, ha voluto esentare da responsabilità solo fino al momento della notizia privata, non

[537] Non mi soffermo sulla terza e quarta (per quest'ultima si è sopra detto della loro sostanziale sovrapponibilità).

[538] Trattandosi di inosservanza di provvedimento del'Autorità per motivi di giustizia, costituirà probabilmente anche violazione dell'art. 650 c.p.

oltre: ne segue che togliere il risarcimento del danno per il periodo successivo e sino a che qualche Autorità ordini la rimozione/disabilitazione, in pratica significherebbe spostare in avanti questo momento. In senso contrario è stato detto che la direttiva lasciava ampi margini per il recepimento, desumibili dai cons. 46 e 48[539]: tuttavia, da un lato, il fatto che tali "disposizioni" siano rimaste nei considerando, senza entrare nell'articolato, le rende di scarso o nullo valore precettivo e, dall'altro, sono comunque così generiche che pare difficile inferirne un riferimento alla comunicazione dell'Autorità, ma, semmai, a procedure di notice and take down finalizzate all'instaurazione di un contraddittorio tra il sedicente soggetto leso e l'uploader[540].

La seconda ipotesi, regolata dall'art. 17 c. 3, è quella per cui l' internet provider è civilmente responsabile del contenuto dei servizi offerti (cioè dei materiali caricati dai suoi utenti)[541] o meglio dei danni cagionati dalla pubblicazione di detti contenuti quando, avuta conoscenza della loro illiceità o dannosità per un terzo, non abbia informato l'Autorità compente. Gli elementi costitutivi della fattispecie sono dunque:

i) che abbia conoscenza: non è richiesto alcun avviso da parte dell'Autorità e dunque basterà la notizia da chiunque proveniente o anche acquisita autonomamente, se l'interessato (il danneggiato) riesca a darne prova. Il provider non è un giudice in sede giudicante, per cui basterà una notizia, da cui una persona di media avvedutezza e preparazione culturale ricavi un giudizio di probabile illiceità o dannosità. Il dubbio, processualmente parlando, non può che giovare al provider, secondo l'ordinario riparto degli oneri probatori. Naturalmente

[539] Tescaro M., *Una proposta ricostruttiva contrastante con il diritto vivente in tema di responsabilità civile dell'internet provider*, cit.,71.

[540] La compatibilità di tali procedure (chiamate *procedural property rules* da Hofmann F.-Kurz F., *Introduction to the <law of remedies>*, in Hofmann F.-Kurz F (eds.), *Law of remedies*, cit., 23) con l'attuale testo della direttiva, però, sarebbe da verificare: questa ha infatti rimandato ad eventuali futuri suoi adeguamenti l'armonizzazione europea sul punto (art. 21). La risposta dovrebbe però essere positiva anche se il punto non può essere qui svolto.

[541] Si tratta cioè di responsabilità per fatto altrui, essendo ovvio che risponde in toto del fatto proprio e del resto non potendosi parlare di <servizi offerti a sé stesso> (anche perché *nemo tenetur se detegere*). Lo si ricava anche dal tenore letterale della disposizione e dalla rubrica dell'art. 17 (la sorveglianza è sulla condotta altrui).

basterà che la comunicazione arrivi al suo indirizzo, non servendo che sia letta e intellettualmente assimilata e ciò anche se si tratta di grande organizzazione: il rischio di ritardata presa di conoscenza, derivante dalle rilevanti dimensioni aziendali, va sopportato dal provider.

ii) carattere illecito o pregiudizievole del contenuto: qui la legge fa una strana distinzione tra illiceità dei contenuti e loro dannosità per un terzo, riprendendo tale quale il criterio direttivo della legge delega. La distinzione tra illiceità (violazione di diritti o situazioni giuridiche altrui) e responsabilità (quando segue un danno ingiusto) è spesso ricordata nelle trattazioni della responsabilità civile ed è probabilmente fondata (può esserci illiceità senza produzione di danno, tanto che è ammessa l'inibitoria preventiva: il tema è però complesso). Va forse intesa nel senso che la conoscenza richiesta basta che riguardi l'illiceità, non servendo che riguardi pure la dannosità per il terzo. La disposizione ricorda la norma generale, per cui nella responsabilità aquiliana vanno risarciti pure i danni non prevedibili, stante il mancato richiamo dell'art. 1225 cc da parte dell'art. 2056: infatti pare ricollegare la responsabilità per mancata comunicazione alla notizia di una qualsiasi illiceità, a prescindere dai danni che da essa prospetticamente potranno sorgere. La formulazione poco sorvegliata o comunque di dubbia consapevolezza –andrebbe verificato- non permette di insistere su questo nesso.

iii) i servizi offerti: si tratta di uno qualunque dei tre tipi di servizi indicati dagli articoli precedenti (v. c. 1): semplice trasporto; memorizzazione temporanea; memorizzazione permanente, anche se è chiaro che la pratica si appunterà soprattutto sugli ultimi due tipi ed anzi sull'ultimo tipo. Come detto sopra, il richiamo proprio ai tre tipi di provider è abbastanza chiaro. Ci si potrebbe allora chiedere cosa succederebbe se l'evoluzione della tecnica o del business enucleasse un diverso tipo (come del resto per le altre norme della dir. 31 o del d. lgs. 70/2003): ci sarebbe da ragionare su un'interpretazione analogica[542].

[542] La dir. già prevedeva ulteriori tipi di servizi come il *linking* e il motore di ricerca da includere in successive revisioni della dir (art. 21 §. 2). Si è notato che alcuni Stati già hanno adottato autonomamente la disciplina pure per essi, col rischio di violare il diritto UE: non certo la dir. 31 ma semmai altre e in particolare la dir. 29/2001 ad es in tema di linking (M. Husovec, *Injunctions aganist*

iv) non ha provveduto ad informare l'Autorità competente: non c'è un termine espresso, ma che ciò debba avvenire prontamente, una volta avutane notizia, è ovvio. Lo impone il concetto di colpa ex art. 2043 o di diligenza ex 1176 cc, se si ravvisa una responsabilità contrattuale (come sarà frequente, dato che a quel punto si tratterà di adempiere ad un obbligo di salvaguardia di una posizione soggettiva ben determinata). Cosa dovrà indicare l'informazione all'Autorità[543]? Dovrà indicare tutte le circostanze a conoscenza del provider, per metterla in grado di procedere con eventuali indagini (copia del file/url/nome e indirizzo dell'utente).

Questa comminazione di responsabilità civile ricorda il dovere di fornire informazioni alle Autorità, posto dal precedente art. 17 c. 2 lett. a). A differenza del rapporto tra la prima ipotesi dell'art. 17 c. 3 e l'art. 16 c. 1 lett. b), sopra ricordata (ove la prima afferma una responsabilità e la seconda una esenzione da responsabilità), nel rapporto tra le norme ora in esame (seconda ipotesi dell'art. 17 c. 3 e art. 17 c.2 sub a)) si nota che entrambe affermano doveri in positivo. In particolare, la prima (art. 17 c. 3, seconda ipotesi) sembra costituire la sanzione -in termini di responsabilità- per la violazione del dovere posto dalla seconda (art. 17 c.2 lett. a). C'è però qualche differenza:

i) nel c. 2 lett. a) la conoscenza concerne "presunte attività o

intermediaries, cit., 51). Respinge l'interpretazione analogica o anche solo estensiva del safe harbour ex art. 16 d. lgs. 70/2003, sulla base del fatto per cui costituirebbe "deroga ad un principio generale di diritto", Trib. Roma n. 14757 del 12.07.2019, RTI c. Dailymotion, Rg 24711/2012, p. 10/11. Il passaggio è impreciso e oscuro. Il giudice prosegue dicendo: <<*Inoltre, visto che l'art. 14 della legge 73/03 che richiama l'art. 16 della direttiva ECOMMERCE introduce una deroga ad un principio generale di respon- abilità aquiliana di cui parte convenuta si vuole avvalere, osserva questo colegio come incombe processualmente alla convenuta DAILYMOTION dare dimostrazione di rientrare nell'ambito applicativo di tale di sposizione e conseguentemente allegare i fatti costitutivi l'eccezione proposta e segnatamente della propria natura di ISP (passivo)*>> A parte l'inversione nella numerazione degli articoli, è azzardato affermare che il safe harbour sia una deroga ad un principio di responsabilità aquiliana: quasi che, al di fuori di esso, la responsabilità stessa vada immancabilmente affermata.

[543] Sfortunatamente la legge non specifica quale sia l'autorità competente. Fatalmente allora si procederà con mail/pec/raccomandate A.R. alla procura della Repubblica e/o alla Polizia Postale competente per territorio rispetto alla sede o agli uffici del provider.

informazioni illecite", mentre nel c.3 sec. ipotesi concerne "il carattere illecito o pregiudizievole del contenuto del servizio". Ebbene, quanto al grado di conoscenza, la differenza è evanescente e potrebbe mancar del tutto; quanto all'oggetto della conoscenza, nel c. 2 si parla di "attività o informazioni illecite" mentre nel c. 3 sec. ipotesi l'illiceità o dannosità è riferita ai contenuti del servizio: anche qui la differenza è tutt'altro che evidente. Potrebbe forse consistere nel fatto che la prima illiceità ha un riferimento soggettivo ("riguardanti un destinatario del servizio"), mentre la seconda ha un riferimento oggettivo ("carattere illecito … del contenuto di un servizio") ovvero anche soggettivo ma dal lato passivo e cioè del soggetto leso ("carattere pregiudizievole per un terzo").

iii) nel c.2 lett. a) non c'è la cennata distinzione tra illiceità e dannosità, presente invece nel c. 3/sec. ipotesi;

iv) nel c.2 lett. a) c'è la locuzione avverbiale "senza indugio", che indica il tempo entro cui si deve informare l'Autorità, mentre questa manca nel c.3/sec. ipotesi.

Quindi per lo più i doveri emergenti (direttamente) dall'art. 17 c.2 lett.a), da un lato, e (indirettamente) dall'art. 17 c.3 seconda ipotesi, dall'altro, si assomigliano, seppur con qualche differenza testuale. Tuttavia eventuali doveri rientranti nella prima norma, che non rientrassero nella seconda, ugualmente sarebbero sanzionati, in caso di loro violazione, dagli artt. 2043 segg. oppure –se si opta per la responsabilità contrattuale- dagli artt. 1218 segg. Nella parte invece, in cui le ipotesi regolate dalle due disposizioni si soprappongono, la seconda (c. 3 sec. ipotesi) è probabilmente inutile, dato che la sanzione di responsabilità civile discende già dalla violazione della prima.

Le fattispecie, di cui al c. 3, non sono presenti nella dir. e sono state introdotte in ossequio alla legge delega (art. 31 c. 1 lett. l) della L. 39 del 2002). Per questo motivo potrebbe in prima battuta pensarsi ad un recepimento difettoso della dir. stessa, ma così non pare sia. O almeno non pare esserlo per il solo fatto di introdurre disposizioni non presenti nella dir., dato che, come noto (art. 288 c. 3 TFUE), la direttiva vincola sul risultato da raggiungere, mentre spetta agli Stati determinare la forma e i mezzi di attuazione. Il problema allora è quello di capire se (non in astratto ma in concreto) la disciplina nazionale de qua abbia questo effetto oppure possa essere incompatibile col risultato imposto dalla dir.

Come si è detto, la dir. pone solo un safe harbour, mentre questa norma dispone in positivo una responsabilità. Non parrebbero allora esserci incompatibilità, dato che il safe harbour non viene toccato nella sua disciplina emergente dalla dir.

Ci si può semmai chiedere se la norma in esame nella sua seconda ipotesi di responsabilità (art. 17 c.3 seconda ipotesi) abbia rispettata la delega, sopra cit., che affermava la responsabilità del provider, quando non avesse agito con diligenza. Infatti la delega imponeva di <<prevedere che il prestatore di servizi è civilmente responsabile del contenuto di tali servizi (…) se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha usato la dovuta diligenza>>[544]. Il d. delegato ha sostituito il riferimento all'uso della dovuta diligenza con il dovere di informare l'Autorità competente: o meglio può dirsi che l'abbia in tale senso precisato e concretizzato[545]. Cosa in sé apprezzabile, data la genericità e superfluità del riferimento alla diligenza, che nulla avrebbe aggiunto all'art 2043 (o al 1176 cc). Ci si può però chiedere se in tal modo rispetti la delega (sempre che questa vada ritenuta da attuare, invece che espunta per interpretatio abrogans a causa della sua genericità, superfluità, mancanza di novità precettiva o simili). La risposta dovrebbe essere positiva, dato che l'informazione all'Autorità costituisce una forma di diligenza in situazioni come quelle de quibus[546]. Il dubbio concerne il fatto che potrebbero ritenersi in tal modo escluse altre modalità di trattamento diligente dell'informazione da parte del provider, delle quali il provider potrà a questo punto disinteressarsi (l'unico suo dovere essendo quello di avvisare l'Autorità): la scelta del decreto delegato, però, non pare criticabile, rientrando nella discrezionalità propria di questa tecnica legislativa.

Concludo ricordando che la recente riforma del copyright (dir. 2019/790), quanto alla comunicazione al pubblico, comporta un

[544] L. 1 marzo 2002 n. 39, art. 31, c.1, lett. l).

[545] La base normativa dell'art. 17 c.3 seconda parte, infatti, pare proprio questa disposizione della legge delega.

[546] Sempre che si ritenga esatto parlare di diligenza per doveri pubblicistici (anche se la loro violazione genera rimedi privatistici).

significativo inasprimento del trattamento giuridico delle piattaforme. Resta da vedere se ciò costituisca spia di un trend generale in tale senso, anziché limitato al copyright e alla proprietà intellettuale[547]. L'impressione è che questo trend sia assai probabile, magari sulla scia intellettuale di opinioni favorevoli a più ampi interventi regolatori delle piattaforme, costituendo la moderazione dei contenuti (speech laws) e il profilo antitrust due aspetti strettamente collegati: si tratta infatti di trend sostenuto da vari stakeholders (dottrina[548], Parlamento europeo[549], unioni sindacali sovranazionali[550], Autorità garanti della concorrenza[551]), anche se non manca qualche opinione

[547] Questa è l'opinione di Frosio G., *It's all linked: how comunication to the public affects internet architecture*, *Computer law § security review*, 2020, § 7, 19 ss

[548] V. ad es. sulla *content moderation*, tra i molti, Langvardt K., *Regulating Online Content Moderation*, cit.: delle possibili soluzioni (p. 1363 ss; l'a. ne elenca quattro: i) definizione legislativa di diritti minimi; ii) obbligo di fornire agli utenti dei *tools* di autodeterminazione, iii) trasparenza sulle effettive policies e procedures adottate; iv) rimanere nello status quo), il lasciare le cose come stanno è quella meno consigliabile (p. 1358 e 1385-1387). La probabilità di regolazione è esposta anche da Suzor N.P., *Lawless. The secret rules that govern our digital lives*, cit., p. 94 ss., con alcuni suggerimenti in proposito. Secondo qualche autore, però, il principio di irresponsabilità dei provider gioca un ruolo esistenziale per loro; per cui introdurre una qualunque forma di responsabilità oggettiva equivarrebbe a decretarne la fine (Bellan A., *Piattaforme, obblighi di monitoraggio e risoluzione delle controversie online*, cit., p. 185). Come modello per la prevenzione di illeciti tramite le piattaforme, propone la disciplina dell'antiriciclaggio nel settore finanziario Carsten U., *A risk-based approach towards infringement prevention on the internet: adopting the anti-money laundering framework to online platforms*, in *International Journal of Law and Information Technology*, Vol. 26/3, 2018, p. 226 ss; non vede rischi di *monopolization* per Facebook, Marchese C., *Debunking the "Big is Bad" Bogeyman: Facebook Benefits Consumers*, Geo. Mason L. Rev., vol. 28/1, 2020, (working copy), sub III, p. 14 ss..

[549] Si vedano gli studi pubblicati nel 2020 per la Commissione *Internal Market and Consumer Protection* del Parlamento UE: - De Streel e altri, *Online Platforms' Moderation of Illegal Content Online*, 23 giugno 2020, cap. 5 *Policy recommendations for the digital services act*, p. 76 ss.; - Schulte-Nölke H.-Rüffer I.-Nobrega C.-Wiewórowska-Domagalska A., The Legal Framework for E-commerce in the Internal Market, maggio 2020, parte 4, p. 35 ss.; - Smith M., Enforcement and cooperation between Member States E-Commerce and the future Digital Services Act, aprile 2020 (spt. sub 6 *Options*, p. 30 ss).

[550] Si v. UNI Global Union and UNI Europa, *Accounting for Workers' Rights When Regulating Amazon & Other Giants*, 2020, passim (spt. pp. 5-6).

[551] v. ad es. il dettagliato report sulle dinamiche concorrenziali, pubblicato da quella inglese CMA-Competition and Markets Authority, *Online platforms and digital advertising. Market study. Final report*, 1 luglio 2020, cap. 7 <*The case*

contraria[552]. Impressione desumibile, dunque, non tanto o non solo dalla disciplina di proprietà intellettuale, quanto, a monte, dal ruolo imprescindibile svolto dalle piattaforme per qualunque flusso comunicativo odierno, stante il loro enorme potere di mercato (e quindi pure di condizionamento sociale in genere). Il che, dato il numero limitatissimo di tali gatekeeper, inevitabilmente porta ad aggravare i loro doveri per la prevenzione delle violazioni: chiunque altro, infatti, ha armi spuntate allo scopo. In sintesi, soprattutto alla luce dei giudizi in tale senso della dottrina e delle ultime mosse dell'UE[553], sta

for a pro-competition regulatory regime>, p. 322 ss., e soprattutto cap. 8 <*Interventions in search, social media, and digital advertising*>, p. 358 ss.

[552] Nordemann J.B., *The functioning of the Internal Market for Digital Services: responsibilities and duties of care of providers of Digital Services*, studio richiesto dalla Commissione *Internal Market and Consumer Protection* del Parlamento UE, maggio 2020, sub 6.6, pp. 46/7 (che auspica semmai l'armonizzazione della responsabilità civile non in generale –irrealistico- ma del cocnetto di *infringer*, p. 30, sub 3.4).

[553] Mi riferisco ad es. a: - Comunicazione della Commissione al Parlamento *Contrastare la disinformazione online: un approccio europeo* del 26.4.2018, COM(2018) 236 final, il cui messaggio implicito è che che, se le piattaforme non provvederanno in modo efficace, seguirà la regolazione (Kaye D., *The global struggle to govern the internet*, cit., p. 100): qui si legge ad es. <<*le piattaforme online che distribuiscono contenuti, in particolare i social media, i servizi di condivisione di video e i motori di ricerca, hanno un ruolo fondamentale nella diffusione e nell'amplificazione della disinformazione online. Finora queste piattaforme non sono riuscite a intervenire adeguatamente e si sono dimostrate impotenti di fronte alla sfida posta dalla disinformazione e dall'uso manipolativo delle loro infrastrutture. Alcune di esse hanno adottato misure moderate per invertire la tendenza alla diffusione di disinformazione online, ma ciò ha interessato un numero limitato di paesi e di utenti. Sorgono inoltre seri dubbi in merito all'efficacia della protezione che la piattaforma è in grado di fornire ai propri utenti contro l'uso non autorizzato dei dati personali da parte di terzi, come hanno recentemente dimostrato le rivelazioni del caso Facebook/Cambridge Analytica, attualmente oggetto di indagine da parte delle autorità di protezione dei dati, riguardante la raccolta non autorizzata di dati personali di milioni di utenti UE dei social media, sfruttati in contesti elettorali*>>, § 1: - consultazione pubblica avviata dalla Commissione UE sul Digital Services Act nel 2020, che probabilmente (quantomeno) ridurrà i benefici da safe harbour per gli ISP: v. parte 1. *How to effectively keep users safer online?*, e parte 3. *What issues derive from the gatekeeper power of digital platforms?*, ma soprattuto la parte 2. *Reviewing the liability regime of digital services acting as intermediaries?*, che probabilmente imporrà l'uso di filtraggi informatici (Keller D., *Facebook Filters, Fundamental Rights, and the CJEU's Glawischnig-Piesczek Ruling*, cit., p. 619); si v. le articolate e interessanti osservazioni di Google in *Digital Services Act package: open public Consultation-Google's submission*, 3 settembre 2020 (soprattutto l'iniziale quadro d'insieme circa la parte II sulla responsabilità degl

diventando probabile un prossimo intervento regolatorio: resta però da vedere in che modo[554] e da parte di chi, dato che, mentre

intermediari, p. 4 ss., e circa la parte III sul loro gatekeeper power, p. 9 ss) e quelle più stringate di Microsoft a firma di Clinge K., *How Europe can take the lead in setting new rules for gatekeeping platforms*, 08.09.2020 (ci sono pure quelle sull'altra consultazione aperta dalla Commissione UE su *Single Market – new complementary tool to strengthen competition enforcement*); - proposta di regolamento UE relativo alla prevenzione della diffusione di contenuti terroristici online 12.09. 2018, COM 2018) 640 final-2018/0331 (COD) (spt. artt.6 e 9). Dubbia invece l'influenza dell'*executive order* 28.05.2020 del Presidente Trump sopra citato, stante l'anomalia (già rilevata: De Gregorio G.-Radu R., *Trump's Executive Order: Another Tile in the Mosaic of Governing Online Speech*, 06.06.2020, medialaws.eu, sub *A Constitutional Paradox*; Venanzoni A.-Monti M., *Il tramonto della frontiera digitale? Note a prima lettura dell'executive order del 28 maggio 2020 emanato per prevenire la censura online da parte dei social media*, in *dirittticomparati.it*, 08.06.2020, p. 7 del.pdf) di un ordine amministrativo che vuole derogare ad un atto legislativo.

[554] Circolano già moltissime proposte. Tuttavia affidarsi sempre più al *monitoring and filtering* automatizzato delle piattaforme (chiamata *collateral censorship* (censura delegata) o *Digital prior restraint* (censura ex ante) da Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, in *UC Davis Law Review* vol. 51, 3, february 2018, 1149 ss, sub II.B, p. 1172 ss.) consoliderà il loro potere e i legami spesso non trasperanti con i Governi (Bloch-Wehba H., *Access to algorithms*, cit., p. 7/8 e 32). Rileva un passaggio da *liability* (responsabilità da negligenza) delle piattaforma a loro *responsibility* (sorta di doveri sociali) Frosio G., *Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility* (October 16, 2017), ceipi.edu, research Paper No. 2017-11, a causa di una delega di fatto da parte degli Stati (*jawboning*), incapaci di provvedere alla prevenzione di illeciti su internet (passim, spt. 10 ss e 16/7). Auspica una regolazione che miri alla trasparenza pubblicamente verificata Douek E., *Verified Accountability*, cit., p. 14 ss (c.d. *public reasoning* delle questioni più significative per incrementarne l'accettzione sociale, oltre ad un incremento dei poteri degli Oversight Boards). Un utile quadro generale delle opzioni regolatorie Keller D., *If Lawmakers Don't Like Platforms' Speech Rules, Here's What They Can Do About It. Spoiler: The Options Aren't Great*, in *techdirt.com*, 09.09.2020 e qui soprauttutto le ultime due, relative all'aumento dei poteri di autodeterminazione degli utenti o con possibilità di settings direttamente in capo a costoro (*empowering users*) o indirettamente, aprendo le API's -*application program interfaces*- (Magic API's) a terze parti (concorrenti o collaboratori delle piattaforme), che potrebbero intervenire a beneficio degli utenti, per incrementarne l'autonomia decisionale sui contenuti desiderati: opzioni teoricamente molto interessanti, ma in pratica difficilmente conseguibili –a meno che le piattaforme lo ritengano per qualche motivo conveniente- sia perché forse presuppongono la conoscenza o divulgazione almeno parziale dei loro segretissimi algoritmi sia perché sconvolgerebbero la gestione della loro fonte di profitti, il microtargeting. Molte proposte all'interno del progetto di *Digital Platform Act* presente nel ponderoso studio di Harold Feld, *The Case for the Digital Platform Act*, cit., sub cap. IV.B, p. 73 ss (esponente di spicco di *PublicKnowledge.org)*. Assai interessanti sono le *Model Rules on Online Platforms* dell'*European law Institute* di Vienna, 2019 (spt., ma non solo, artt-.

gli intermediari digitali sono ubiqui, il potere normativo è invece rimasto statale (al massimo europeo)[555].

19-24 e relativi commenti), esaminate da Busch C.-Dannemann G.-Schulte Nolke H.-Wiewiórowska-Domagalska A.-Zoll F., *The ELI model rules on online platforms*, in *Journal of European Consumer and Market Law*, 2020/2, p. 61 ss (Zoll è uno dei project reporters, si legge nel sito ELI).

[555] Per quanto detto alla nota precedente, è possibile che anche qui, come per il GDPR, l'UE farà da battistrada.