

VERSO UNA FORMA DI POLIZIA PRIVATA NELLO SPAZIO DIGITALE? L'INEDITO RUOLO DEI PROVIDER NELLA DISCIPLINA TEDESCA DEI SOCIAL NETWORK^(*)

di Johanna Rinceanu

SOMMARIO: I. Introduzione. – II. Legge per il miglioramento dell'applicazione del diritto nei *social network* (*Netzwerkdurchsetzungsgesetz*: NetzDG). – 1. Origine e obiettivi. – 2. Cambiamenti nella cultura del dibattito. – a) *Hate speech*. b) *Fake news* e disinformazione. – 3. Contenuto essenziale del NetzDG. – 4. Autoregolamentazione regolata o censura autoregolamentata? – III. Compatibilità con i diritti fondamentali e umani. – 1. Libertà di opinione. – 2. Diritto allo sviluppo della personalità, in generale, e diritto all'autodeterminazione informativa, in particolare. – 3. Libertà della professione. IV. Legge per combattere l'estremismo di destra e i crimini d'odio. – 1. Obiettivo. – 2. Contenuti essenziali. – a) Modifiche al codice penale – b) Modifiche al NetzDG – 3. Dubbi di costituzionalità e osservazioni critiche. – V. Conclusioni.

I. INTRODUZIONE.

Migliaia di sostenitori di Donald Trump si sono riuniti davanti alla Casa Bianca il 6 gennaio 2021 a Washington D.C. per ascoltare il discorso del 45° Presidente degli Stati Uniti d'America "Save America March"¹. Incitati da slogan come «*we will stop the steal*», «*we fight like hell*» e «*we are going to the Capitol*», hanno marciato verso il Campidoglio. Centinaia di manifestanti hanno poi preso d'assalto il Campidoglio, mentre al Congresso i deputati legittimavano il futuro 46° Presidente degli Stati Uniti d'America. Cinque persone, quattro manifestanti e un agente di polizia, hanno perso la vita nell'assalto al Campidoglio.

Prima di ciò, per anni Trump aveva riempito il suo *account* Twitter @realDonaldTrump con innumerevoli *post* che incitavano all'odio. Teorie cospirative, disinformazione e affermazioni infondate – di recente su presunti brogli elettorali e sulla presunta illegittimità del neo eletto Presidente – sono state seguite da oltre 87 milioni di persone su Twitter. Naturalmente, attraverso la rete questi *post* potevano essere letti anche in Germania e in Italia e, presumibilmente, anche dai cittadini dei due Stati che si trovavano negli Stati Uniti. In linea di principio, non sarebbe del tutto azzardato invocare l'art. 414 del codice penale italiano o il § 111 del codice penale tedesco (StGB), con i consueti problemi di collisione tra sistemi giuridici nazionali nel cyberspazio

^(*) Contributo destinato agli *Scritti in onore di Antonio Fiorella*, a cura di M. CATENACCI, N. D'ASCOLA, R. RAMPIONI, Roma Tre Press ed., Roma 2021.

¹ Il discorso di Trump del 6 gennaio 2021 può essere letto su <https://www.independent.co.uk/news/world/americas/us-election-2020/trump-speech-6-january-transcript-impeachment-b1786924.html>.

globale. Ma tali problemi sono oggi acuiti dal fatto che, in molti casi, l'attuazione delle norme nazionali non è più di competenza delle pubbliche autorità, ma di attori privati.

Inizialmente, Twitter e Facebook hanno pubblicato avvertimenti circa le falsità presenti in vari *post* di Trump, e in alcuni casi ne hanno anche limitato la diffusione. Dopo i tumulti in Campidoglio, l'*account* Twitter di Trump è stato bloccato dal *service provider*, prima per 12 ore e poi definitivamente. A ciò ha fatto seguito l'ulteriore sospensione dei suoi *account* da parte di Facebook, Instagram e Snapchat. La ragione addotta è stata la violazione dei regolamenti e delle linee guida delle piattaforme *online*, con il rischio di un ulteriore incitamento alla violenza².

Il blocco dell'*account* di Donald Trump da parte di un fornitore di servizi informatici è stato criticato sia negli Stati Uniti che a livello internazionale. In particolare, la Cancelliera tedesca ha definito il blocco come un attacco alla libertà di opinione e ne ha messo in dubbio il fondamento giuridico. Ma proprio in Germania, il potere esecutivo ed il potere legislativo si mostrano molto meno riluttanti ad intervenire. Infatti, con la "Legge per il miglioramento dell'applicazione del diritto nei *social network*" (*Netzwerkdurchsetzungsgesetz*, di seguito: NetzDG), la Germania ha compiuto un tentativo di regolamentazione statale del "mondo senza confini di Internet"³, condotto, però, mediante l'investitura legale di soggetti privati, quali sono gli *internet provider*, nel ruolo di controllori della sua pratica attuazione. E all'orizzonte si profilano riforme improntate ad un crescente rigore.

Di seguito, si fornirà anzitutto una lettura critica del NetzDG (II.), prestando particolare attenzione alla sua dubbia compatibilità con i diritti fondamentali e con i diritti umani spettanti a vari soggetti attivi nello spazio digitale (III.). In un secondo momento, ci si soffermerà, sempre in chiave critica, sulla "Legge per combattere l'estremismo di destra e i crimini d'odio", che sostanzialmente prevede l'inasprimento di alcune disposizioni del codice penale e del NetzDG (IV.). Nelle conclusioni si azzarderà qualche previsione sul futuro della *governance* di *internet* in relazione ai diritti umani (V).

II. LEGGE PER IL MIGLIORAMENTO DELL'APPLICAZIONE DEL DIRITTO NEI SOCIAL NETWORK (*NETZWERKDURCHSETZUNGSGESETZ: NETZDG*).

1. Origine e obiettivo.

Come evidenziato dalla relazione che accompagna il NetzDG, il mutamento del discorso pubblico sui *social network* e la "brutalizzazione della cultura del dibattito"⁴

² Dopo l'assalto al Campidoglio, Twitter aveva anche cancellato più di 70.000 account legati all'estrema destra e all'ideologia cospirazionista del movimento QAnon.

³ KÜLLMER, *Die Regulierung von Internetinhalten in demokratischen Systemen – Deutschland, Großbritannien, USA*, Wiesbaden, 2019, p. 2.

⁴ BT-Drucks. 18/12356, p. 13.

attraverso contenuti in internet “aggressivi, offensivi e spesso odiosi”⁵, che talvolta conducono ad una vittimizzazione violenta nel mondo reale, hanno spinto il legislatore tedesco a migliorare l’applicazione del diritto nei *social network*⁶.

Con il complesso di norme comprese nel NetzDG, la lotta contro i crimini d’odio *online* e le *fake news*, sinora affidata al senso di auto-responsabilità dei fornitori di servizi informatici e alla loro autodisciplina, viene assoggettata alla legge. Il NetzDG, entrato in vigore il 1° ottobre 2017, ha lo scopo di eliminare i pericoli per la sicurezza pubblica e di indurre un cambiamento nella “cultura del dibattito”⁷ sui *social network* mediante il supporto di attori privati.

2. Cambiamento della cultura del dibattito.

Il cambiamento della cultura del dibattito *online* ha molte sfaccettature. È osservabile una tendenza alla degenerazione violenta: nei *social* dilagano intimidazioni, denigrazione, diffamazioni, insulti, molestie, minacce e persino “scenari espliciti di omicidi e stupri”⁸. Inoltre – e in modo non irrelato da siffatta tendenza –, si constata un rapido aumento di voci e di false informazioni, in grado di condurre ad un cambiamento complessivo del clima politico-sociale. Realtà e realtà virtuale rischiano di fondersi⁹.

Con il pretesto dell’anonimato in internet, il libero sviluppo della personalità in ambito digitale (*digitale Selbstentfaltung*) si trasforma in una rimozione digitale della capacità di autocontrollo (*digitale Selbstentfesselung*)¹⁰. È quanto dimostrano i due fenomeni sociali che qui s’intende richiamare: l’*hate speech* e le *fake news*.

a) *Hate speech*

L’*hate speech* (“discorso d’odio”) è un fenomeno globale; tuttavia, a livello internazionale non ne esiste ancora una definizione giuridicamente vincolante. Nel 1997,

⁵ BT-Drucks. 18/12727, p. 2.

⁶ CEFFINATO, *Zur Regulierung des Internet durch Strafrecht bei Hass und Hetze auf Onlineplattformen*, in ZStW 132, 2020, p. 547, osserva a questo proposito, tuttavia, che “[l]e statistiche sulla criminalità di polizia [...] non confermano l’aumento dei crimini motivati dall’odio attraverso Internet percepito dall’opinione pubblica e dai politici. Mentre nel 2018 sono stati registrati poco più di 8.000 cosiddetti crimini d’odio - con una recente tendenza solo lievemente al rialzo - il numero dei cosiddetti messaggi d’odio è in realtà diminuito, passando da circa 3.000 nel 2016 a poco meno di 1.500 nel 2018”.

⁷ MÜLLER-FRANKEN, *Netzwerkdurchsetzungsgesetz: Selbstbehauptung des Rechts oder erster Schritt in die selbstregulierte Vorzensur? – Verfassungsrechtliche Fragen*, in AfP 1/2018, pp. 1-2.

⁸ FLEISCHHACK, *Der “Hass” der vielen Formen*, in Kaspar, Gräßler, Riffi (Hrsg.), *Online Hate Speech - Perspektiven auf eine neue Form des Hasses*, Düsseldorf,-München, 2017, p. 24.

⁹ HAJOK, SELG, *Kommunikation auf Abwegen? Fake News und Hate Speech in kritischer Betrachtung*, in JMS-Report, August 4/2018, p. 2.

¹⁰ KOLANY-RAISER, WERNER, *Fake News und Hate Hate Speech*, in ABIDA Dossier, Juni 2018, p. 1, notano che internet “abbassa la soglia di inibizione [dato] il basso rischio di persecuzione”. Tuttavia, gli Autori evidenziano allo stesso tempo che l’anonimato su Internet può anche essere stimolante per lo scambio di opinioni.

il Comitato dei Ministri del Consiglio d'Europa ha rivolto una Raccomandazione agli Stati membri per combattere i discorsi d'odio – specialmente quelli diffusi attraverso i media –, che incitano all'odio razziale, alla xenofobia, all'antisemitismo e a tutte le forme di intolleranza, minando la sicurezza democratica, la coesione culturale e il pluralismo¹¹. Nella Raccomandazione, con la locuzione "discorso d'odio" si intendeva "qualsiasi espressione che promuove, incita, incoraggia o giustifica l'odio razziale, la xenofobia, l'antisemitismo o altre forme di odio basate sull'intolleranza, compresa l'intolleranza espressa sotto forma di nazionalismo aggressivo ed etnocentrismo, la discriminazione e l'ostilità verso le minoranze, gli immigrati e le persone di origine immigrata"¹².

A tutt'oggi il diritto tedesco non prevede una definizione del concetto. Questa lacuna è dovuta principalmente alla difficoltà di distinguere tra la libertà di espressione, da tutelare, e le affermazioni potenzialmente riconducibili alla nozione di "discorso d'odio". Neppure il NetzDG ha adottato il termine "*Hassrede*" (l'equivalente tedesco di "discorso d'odio"), nel senso della citata Raccomandazione del Comitato dei Ministri del Consiglio d'Europa, né ha introdotto una propria definizione giuridica. Il § 1, comma 3 del NetzDG ha preferito invece fare rinvio al reato di cui al § 130 StGB, il cui comma 1 punisce la condotta di "istigazione all'odio" nei confronti di un gruppo nazionale, razziale, religioso o di un gruppo determinato dalla sua origine etnica, contro parti della popolazione o contro un individuo, a causa della sua appartenenza a uno dei suddetti gruppi o ad una parte della popolazione. Per il legislatore tedesco, dunque, il discorso d'odio diviene illecito – e non è più costituzionalmente tutelato –, ogni qualvolta raggiunga l'intensità dell'"istigazione all'odio". Secondo la giurisprudenza della Corte federale di giustizia (BGH), per "odio", ai sensi del § 130 StGB, s'intende un "atteggiamento ostile, emotivamente accentuato, diretto ad una parte di popolazione, che oltrepassi il semplice rifiuto o il disprezzo"¹³. L'"istigazione" (all'odio) è inoltre definita come influsso sui sensi, sulle passioni ed anche sull'intelletto, oggettivamente idoneo e soggettivamente diretto a suscitare odio¹⁴. Tuttavia, non è d'immediata evidenza quando l'incitamento ad un atteggiamento ostile superi la soglia della mera induzione al rifiuto o al disprezzo¹⁵. Per tanto, il richiamo del NetzDG (tra gli altri) agli §§ 130 e 111 StGB è poco utile, né aiuta i *service provider* ad orientarsi nella prassi.

Affinché questi ultimi possano attivarsi contro l'*hate speech* in rete, sarebbe fondamentale elaborare una definizione del fenomeno attenta alla prassi, che poi possa essere ripresa dal testo di legge. I gestori dei *social network* dovrebbero essere messi in condizione di riconoscere quando determinati contenuti, non solo trasgrediscono la decenza e il rispetto, esprimendo critiche taglienti, ma si trasformano in veri e propri contenuti illeciti e se del caso punibili.

¹¹ Raccomandazione R (97) 20 del Comitato dei Ministri del Consiglio d'Europa del 30 ottobre 1997, disponibile sul sito <http://www.egmr.org/minkom/ch/rec1997-20.pdf> (Ultimo accesso: 10 febbraio 2021).

¹² Si veda Raccomandazione Nr. R (97) 20, cit.

¹³ Si veda BGH, Urt. v. 27.7.2017, 3 StR 172/17; BGH, Urt. v. 3.4.2008, 3 StR 394/07; STERNBERG-LIEBEN, SCHITTENHELM, § 130, Rd. 5a, in Schönke, Schröder, *StGB – Strafgesetzbuch Kommentar*, 30. Aufl. 2019.

¹⁴ STERNBERG-LIEBEN, SCHITTENHELM, § 130, Rd. 5, in Schönke, Schröder, cit.

¹⁵ HÖRNLE, *Grob anstößiges Verhalten. Strafrechtlicher Schutz von Moral, Gefühlen und Tabus*. Frankfurt am Main, 2005, p. 302.

Secondo un'opinione diffusa, il "discorso d'odio" *online* è inteso come un linguaggio dispregiativo e istigatorio contro *gruppi di popolazione* con determinate caratteristiche¹⁶. I colpevoli e le vittime di solito non si conoscono personalmente. Attraverso questa pratica, intere categorie di persone sperimentano il razzismo, l'antisemitismo, il razzismo anti-musulmano, il sessismo, l'omotransfobia, l'antiziganismo, l'abilismo¹⁷, il classismo, il lookismo¹⁸ e l'ageismo¹⁹. E l'elenco non è esaustivo, perché in pratica non c'è "nessuna caratteristica umana [che] non possa essere resa oggetto di odio"²⁰. Il discorso d'odio colpisce anche quei *gruppi che si battono* in favore delle minoranze e contro il loro ostile isolamento, come i giornalisti²¹, i politici e gli avvocati per i diritti umani.

L'*hate speech*, come forma di ostilità umana e di incitamento all'odio in rete, ha un messaggio intrinseco, che mira a polarizzare la società e può portare ad aggressioni nel mondo reale²². I reati attualmente impiegati per perseguire questo fenomeno, almeno in Germania, sono, oltre al già citato reato di cui al § 130 StGB, l'ingiuria (§ 185 StGB), la diffamazione (§ 186 StGB), la menzogna diffamatoria (§ 187 StGB), la diffamazione e menzogna diffamatoria contro personaggi della vita politica (§ 188 StGB) e il pubblico incitamento a commettere reati (§ 111 StGB)²³.

b) *Fake news* e disinformazione

Il XXI secolo non è solo l'era della digitalizzazione. È anche l'era della post-fattualità: strumenti come "*fake news*", "fatti alternativi"²⁴ e verità "soggettive" o

¹⁶ SCHMITT, *Online Hate Speech: Definition und Verbreitungsmotivation aus psychologischer Perspektive*, in KASPAR, GRÄBLER, RIFFI (Hrsg.), *Online Hate Speech – Perspektiven auf eine neue Form des Hasses*, Düsseldorf, München, 2017, p. 51; MEIBAUER, *Hassrede – von der Sprache zur Politik*, in Meibauer (Hrsg.), *Hassrede/Hate Speech – Interdisziplinäre Beiträge zu einer aktuellen Diskussion*, 2013, p. 1; HAJOK, *Hate Speech. Hass und Hetze im Netz als Thema des Kinder- und Jugendmedienschutzes*, in JMS-Report – Februar 1/2017, p. 2.

¹⁷ Per "abilismo" si intende la discriminazione nei confronti delle persone con disabilità fisica o mentale.

¹⁸ Per le diverse forme di "Hate Speech" vedi BUNDESZENTRALE FÜR POLITISCHE BILDUNG, *Was ist Hate Speech?*, disponibile sul sito <https://www.bpb.de/252396/was-ist-hate-speech> (Ultimo accesso: 10 febbraio 2021).

¹⁹ L'"ageismo" è inteso come una forma di discriminazione sociale ed economica contro gli anziani.

²⁰ MEIBAUER, *Hassrede*, cit., p. 2.

²¹ OBERMAIER, HOFBAUER, REINEMANN, *Journalists as targets of hate speech – How German journalists perceive the consequences for themselves and how they cope with it*, in SCIM 4/2018, pp. 502-502, richiamano l'attenzione sul fatto che i "discorsi sull'odio" possono intimidire i giornalisti e quindi influenzare la qualità del reportage.

²² BUNDESZENTRALE FÜR POLITISCHE BILDUNG, *Was ist Hate Speech?*, cit.

²³ Negli Stati Uniti d'America, invece, l'"hate speech" rientra nel Primo Emendamento della Costituzione (*freedom of speech*) e quindi non può (di norma) essere perseguito penalmente. Vedi VALERIUS, *Hasskriminalität – Vergleichende Analyse unter Einschluss der deutschen Rechtslage*, in ZStW 132, 2020, p. 679. Per un confronto tra l'approccio tedesco e quello americano alla regolamentazione dell'*hate speech*, vedi HAUPT, *Regulating Hate Speech – Damned If You Do and Damned If You Don't: Lessons Learned from Comparing the German and U.S. Approaches*, in 23 B.U.INT'L L.J. (2005), pp. 299 ss.

²⁴ Il termine "*alternative facts*" risale all'americana Kellyanne Conway, consigliere del Presidente degli Stati Uniti Donald Trump dal 2016 al 2020, la quale, in un'intervista del 2017 su *Meet the Press della NBC* - per giustificare le false dichiarazioni rilasciate dall'allora addetto stampa della Casa Bianca Sean Spicer sulle

“percepiti” stanno scalzando “criteri fattuali come la ricerca, l'evidenza probatoria e l'assenza di contraddizioni”.²⁵ I fatti e la finzione si fondono senza soluzione di continuità.

La diffusione di falsità – la menzogna in quanto tale²⁶ – non è vietata²⁷. Le *fake news* ("notizie false"), tuttavia, non sono solo “falsità”, ovvero segnalazioni o informazioni false, diffuse in rete da individui singoli e soggetti privati, soprattutto attraverso i social media. Per loro essenza, le *fake news* costituiscono una disinformazione sistematica, ossia un insieme di contenuti liberamente inventati o di reinterpretazioni di fatti indiscussi, deliberatamente creati e diffusi in formato digitale, al fine di fuorviare e quindi di manipolare individui, gruppi e organizzazioni²⁸.

La manipolazione digitale del processo di formazione delle opinioni altrui mira a cambiare il comportamento nella vita quotidiana; può portare a danni alla reputazione, all'esclusione di persone o gruppi, ad influenzare alcune scelte politiche come il voto, o può cagionare danni di tipo patrimoniale o lesioni di altri interessi degni di protezione nel mondo reale. Non di rado si suscitano emozioni come invidia, rabbia e paura, e si fomentano ed acquiscono i pregiudizi. Nello spazio digitale, di cui deliberatamente si abusa in questo modo, può accumularsi una narrazione mendace – una "mentitiva" in opposizione alla “narrativa”, come è stato scritto²⁹ – che, illustrando una particolare visione del mondo, reca in sé il potenziale per scuotere le fondamenta della democrazia, se posta alla base di decisioni collettive³⁰. Si pensi, nuovamente, ai recenti avvenimenti negli Stati Uniti. Ma un esempio analogo è offerto, in Germania, dagli esponenti del c.d.

dimensioni della folla durante l'inaugurazione di Trump davanti al Campidoglio – dichiarò che si trattava di “*alternative facts*”; in ragione del fatto che, dopotutto, non c'era modo di quantificare con certezza le folle.

²⁵ ZIMMERMANN, KOHRING, *Aktuelle Desinformation – Definition und Einordnung einer gesellschaftlichen Herausforderung*, in: Hohlfeld, Harnischmacher, Heinke, Lehner, Sengl (Hrsg.), *Fake News und Desinformation – Herausforderungen für die vernetzte Gesellschaft und die empirische Forschung*, Baden-Baden 2020, p. 31.

²⁶ SCHÜNEMANN, *Gefährden Fake News die Demokratie, wächst aber im Strafrecht das Rettende auch?*, in GA 10/2019, p. 621.

²⁷ SCHÜNEMANN, *Gefährden Fake News die Demokratie*, cit., p. 629, sottolinea, [...] „dass der die Demokratie konstituierende Meinungskampf in der Gesellschaft nicht von der Staatsmacht kontrolliert werden darf. Es muss deshalb einen Freiraum auch für waghalsige Behauptungen geben, weshalb es ausgeschlossen ist, die einzelne Falschbehauptung als solche zu kriminalisieren. Und mehr noch: Es ist geradezu eine Naturnotwendigkeit für eine funktionierende Demokratie, dass die offiziell h.M. herausgefordert wird, sich zu bewähren und beweisen.“

²⁸ HAJOK, SELG, *Kommunikation auf Abwegen? Fake News und Hate Speech in kritischer Betrachtung*, in JMS-Report, August 4/2018, p. 3. PAUL, *Truth isn't Truth – Fake News und Real News in der Ära Trump*, Münster 2019, p. 96, riporta che il governo britannico ha vietato il termine "fake news" dal suo vocabolario ufficiale nel 2018, in quanto questo termine è stato assegnato alla scena di destra come termine da combattimento. Invece di "fake news", è stato ufficialmente usato il termine "desinformation". Con ciò si intende "la creazione e la condivisione deliberata di informazioni false e/o manipolate che hanno lo scopo di ingannare e fuorviare il pubblico, sia allo scopo di causare danni, sia per fini politici, personali o finanziari".

²⁹ SCHÜNEMANN, *Gefährden Fake News die Demokratie*, cit., p. 630, parla a tal riguardo di una "Mentitiv" come di una "narrazione complessa, generalmente usata e creduta dopo essere entrata in uso, ma su cui si è mentito".

³⁰ SCHÜNEMANN, *Gefährden Fake News die Demokratie*, cit., p. 630.

Querdenkerbewegung, cioè del movimento di pensiero anticonformista o "trasversale", che mette sistematicamente in discussione i pericoli dell'attuale pandemia.

Con riguardo alla questione dell'applicabilità del diritto penale alle *fake news*, occorre anzitutto distinguere se la notizia "falsa" è una *falsa dichiarazione di fatto* o un'*opinione*. Quest'ultima non rientra nel concetto di *fake news*, trattandosi notoriamente dell'espressione di un convincimento personale, protetta quale diritto fondamentale³¹. Un'opinione non è suscettibile di prova. Le affermazioni di fatto, invece, si riferiscono a dati della realtà, che possono essere provati o smentiti. Esse rientrano nell'ambito della tutela della libertà di opinione, solo nella misura in cui sono, o possono essere, un prerequisito della formazione di un'opinione³². Questa classica demarcazione tra fatti e opinioni, secondo il criterio della dimostrabilità, implica che "la libertà di commentare i fatti o di comunicarli e diffonderli merita una protezione inferiore, dal punto di vista dei diritti fondamentali, della libertà di prendere posizione sul mondo"³³. Questo assunto è invero contestato da chi osserva che il grado di dimostrabilità di un discorso non dovrebbe incidere sulla tutela della libertà di tenerlo: la distinzione tra un'affermazione di fatto e un'opinione, per tanto, non dovrebbe basarsi sul contenuto dell'affermazione, ma piuttosto sul modo in cui essa viene espressa³⁴.

In ogni caso, accuse deliberatamente o palesemente non veritiere non godono della tutela della libertà di espressione³⁵. Se un'accusa fondata su dati di fatto irreali sia punibile, dipende dal suo essere diretta ad una persona o a un gruppo di persone concrete, o dall'essere un messaggio falso a contenuto generico, cioè senza riferimenti a persone o gruppi di persone concrete. Quest'ultima ipotesi è, in linea di principio, sottratta alla punizione³⁶, a meno che non si tratti della negazione

³¹ Se l'espressione di opinioni offende l'onore di una persona, può essere integrato il reato di diffamazione, se sono soddisfatti i requisiti richiesti dal §185 StGB.

³² Si veda BVerfGE 61, 1 <8>; BVerfGE 90, 241 <247>.

³³ BUCHHEIM, *Rechtlicher Richtigkeitsschutz – Zugleich ein Beitrag zur Unterscheidung von Meinungen und Nachrichten im Rahmen des Art. 5 Abs. 1 GG*, in *Der Staat*, 59, 2020, p. 14.

³⁴ BUCHHEIM, *Rechtlicher Richtigkeitsschutz*, cit., p. 14.

³⁵ BVerfGE 54, 208 <219>; BVerfGE 61, 1 <8>; BVerfGE 90, 241 <247>.

³⁶ L'AG Mannheim si è pronunciata diversamente, con sentenza del 07 gennaio 2019 – 20 Cs 806 Js 10181/18 –, condannando un blogger ad una multa di 12.000 euro ai sensi del § 126, commi 1 e 2, in combinato disposto con il § 20, comma 1 PresseG BW (Legge sulla stampa del Baden Württemberg), per aver disturbato la pace pubblica, pubblicando intenzionalmente notizie false su un attacco terroristico in un blog collegato. Il 25 marzo 2018 alle 3:47 del mattino, il blogger aveva scritto un articolo sul suo blog locale su internet, presentandolo da una prospettiva oggettiva e deliberatamente contro l'evidenza, ed utilizzando titoli del seguente tenore: "136 morti - 237 feriti - caos in città - unità antiterrorismo in azione" e "Massiccio attacco terroristico a Mannheim", in cui parlava del più grande attacco terroristico in Europa occidentale fino ad oggi. Inoltre, riferiva che circa 50 aggressori armati di machete e altri coltelli avevano aggredito persone accorse a feste che si stavano svolgendo nel centro di Mannheim, causando un bagno di sangue di proporzioni apocalittiche, e che venti aggressori erano ancora in circolazione in città. Il blogger riferiva anche che era stato imposto un blackout sulle notizie, e che i canali dei social media erano stati volutamente bloccati per evitare il panico di massa. Solo dopo 20 paragrafi e un c.d. paywall, si poteva apprendere che l'articolo era fittizio. La pagina del blogger con l'articolo è stata collegata sia a un account Facebook che a un account Twitter, e gli utenti dei rispettivi social media hanno avuto accesso per un totale di oltre 20.000 volte. Ci fu poi un numero molto elevato di risposte all'articolo da parte di utenti preoccupati e spaventati.

dell'Olocausto³⁷. Se una persona o un gruppo di persone concrete sono vittime di una falsa accusa di fatto e se sono denigrate o calunniate, possono applicarsi le fattispecie di ingiuria (§ 185 StGB), diffamazione (§ 186 StGB), menzogna diffamatoria (§ 187 StGB) e diffamazione e menzogna diffamatoria contro personaggi della vita politica (§ 188 StGB).

3. Contenuto essenziale del NetzDG

Il NetzDG si rivolge ai "provider di social network" con oltre due milioni di utenti registrati in Germania (§ 1, comma 2 NetzDG). Cosa esattamente s'intenda per "social network", lo spiega il § 1, comma 1 NetzDG: si tratta di "fornitori di servizi telematici che, con l'intento di trarne profitto, gestiscono piattaforme internet finalizzate a che gli utenti condividano qualsiasi contenuto con altri utenti o lo rendano accessibile al pubblico". Sono esplicitamente escluse dalla legge le piattaforme con contenuti giornalistico-editoriali, di cui sia responsabile il fornitore di servizi internet, nonché la comunicazione individuale e la comunicazione di un gruppo chiuso come i servizi Messenger o i gruppi WhatsApp. Sono dunque interessati *providers* del calibro di Google, Facebook, YouTube, Twitter e Instagram.

Tali fornitori di servizi sono obbligati dal NetzDG, in quanto *privati*, ad istituire un sistema trasparente di gestione dei reclami (in base a "regole di *compliance*") concernenti contenuti illeciti. I "contenuti illeciti" rilevanti sono elencati, in modo tassativo, dal § 1, comma 3 del NetzDG attraverso un catalogo di reati³⁸. La procedura di gestione dei reclami deve garantire che il fornitore prenda immediatamente atto del reclamo, verificando se il contenuto in esso riportato sia illecito, se debba essere rimosso o se debba esserne bloccato l'accesso. I contenuti manifestamente illeciti devono essere rimossi o l'accesso ad essi deve essere bloccato entro 24 ore dalla ricezione del reclamo; per i contenuti *non* manifestamente illeciti vale di regola un termine di sette giorni. Il

Cittadini preoccupati hanno chiamato la polizia di Mannheim per informarsi sui familiari residenti in quella città. L'AG Mannheim ha considerato tale condotta un disturbo della quiete pubblica, posto in essere simulando l'imminente realizzazione di un assassinio, un omicidio colposo o lesioni personali gravi.

³⁷ Ai sensi del § 130, comma 3 StGB.

³⁸ § 1, comma 3 NetzDG elenca i seguenti reati: § 86 StGB (Diffusione di mezzi di propaganda di organizzazioni incostituzionali), § 86a StGB (Uso di contrassegni di organizzazioni incostituzionali), § 89a StGB (Preparazione di un grave atto di violenza che mette in pericolo lo Stato), § 91 StGB (Istruzioni per commettere un grave atto di violenza che mette in pericolo lo Stato), § 100a StGB (Falsità a scopo di tradimento della Patria), § 111 StGB (Pubblico incitamento a commettere reati), § 126 StGB (Turbativa della pace pubblica mediante la minaccia di reati), §§ 129-129b StGB (Formazione di associazioni criminali, Formazione di associazioni terroristiche, Associazioni criminali e terroristiche all'estero), § 130 StGB (Istigazione all'odio), § 131 StGB (Apologia della violenza), § 140 StGB (Remunerazione ed apologia di reati), § 166 StGB (Vilipendio di culti, comunità religiose e associazioni ideologiche), § 184b StGB i.V.m. § 184d StGB (Distribuzione, acquisizione e possesso di scritti pedopornografici in relazione alla messa a disposizione di contenuti pornografici per mezzo di trasmissioni radiotelevisive o telematiche), §§ 185-187 StGB (Ingiuria, Diffamazione, Menzogna diffamatoria), § 201a StGB (Violazione della sfera intima e dei diritti della personalità attraverso ripresa di immagini), § 241 StGB (Minaccia) o § 269 StGB (Falsificazione di dati probatori).

NetzDG, però, non specifica cosa s'intenda per "contenuto manifestamente illecito". In caso di cancellazione, il contenuto deve essere custodito a fini probatori e conservato per un periodo di dieci settimane. Infine, il fornitore di servizi informatici deve informare senza indugio il reclamante (che non necessariamente coincide con la persona offesa dal contenuto) e l'utente (nel senso di autore del contenuto) di ogni decisione, di cui deve anche fornire una motivazione (§ 3 NetzDG).

La trasparenza è assicurata dall'obbligo del *provider* di pubblicare nel *Bundesanzeiger* e nella propria *homepage*, ogni sei mesi (quindi ad intervalli regolari), un rapporto in lingua tedesca sulla gestione dei reclami relativi ai contenuti illeciti individuati nelle proprie piattaforme (§ 2 NetzDG). Se un fornitore viola i propri obblighi di gestione dei reclami e di notifica ai sensi dei §§ 2 e 3 NetzDG, "omettendo di istituire un sistema di gestione dei reclami, intenzionalmente o per negligenza, o istituendolo in modo inadeguato, non ponendo rimedio alle carenze organizzative o non rispettando i requisiti di legge per la gestione dei reclami per un periodo di tempo non trascurabile"³⁹, si configura un illecito amministrativo, punito con una sanzione pecuniaria fino a cinquecentomila euro, in casi eccezionali fino a 5 milioni di euro (§ 4 NetzDG). Grazie ad un richiamo al § 30, comma 2, 3° periodo della Legge sull'illecito amministrativo (OWiG), contenuto nel § 4, comma 2 NetzDG, la sanzione pecuniaria massima è aumentata di dieci volte per le fattispecie previste dal NetzDG. Poiché gli operatori del settore sono di solito persone giuridiche, l'entità della sanzione è di fatto elevata fino a cinquanta milioni di euro. Apposite linee guida, emanate dalle autorità amministrative ai sensi del § 4, comma 4 NetzDG, dovrebbero garantire una maggiore trasparenza nella commisurazione della sanzione, che è correlata alle dimensioni del fornitore, al numero dei suoi utenti, come pure alle circostanze e alle conseguenze del fatto⁴⁰. Ma tale espediente non è in grado di assolvere appieno questa funzione.

Infine, il NetzDG impone ai fornitori l'obbligo di nominare, a livello nazionale, un rappresentante autorizzato e un addetto al rilascio di informazioni per le richieste provenienti dalle autorità nazionali competenti per il perseguimento dei reati, indicando queste figure sulla propria piattaforma in modo facilmente riconoscibile e direttamente accessibile (§ 5 NetzDG). Anche questi obblighi sono soggetti a sanzioni pecuniarie.

4. Autoregolamentazione regolata o censura autoregolamentata?

Con il NetzDG è stato introdotto un sistema di "*autoregolamentazione regolata*" (§ 3, comma 6 NetzDG), incentrato sull'istituzione di un organismo incaricato di verificare i contenuti online non manifestamente illeciti.

Ciò consente ai fornitori di servizi informatici, in caso di dubbia liceità di un contenuto, di delegare la decisione sulla sua cancellazione o blocco a tale organismo di verifica, ispirato al modello della autoregolamentazione regolata. Tuttavia, la decisione

³⁹ BT-Drucks. 18/12356, p. 12.

⁴⁰https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/NetzDG_Bu%C3%9Fgeldleitlinien.pdf?__blob=publicationFile&v=3.

può essere delegata solo in singoli casi controversi, sempre che si tratti di contenuti “semplicemente” illeciti (cioè non “manifestamente” illeciti), e non sistematicamente. L’esercizio sistematico di questa facoltà si esporrebbe a sua volta a sanzioni pecuniarie.

Nella pratica, a fronte di un elevato numero di valutazioni da effettuare, i fornitori sono per lo più abbandonati a loro stessi. Per un verso, bisogna considerare che da anni essi esercitano, in tutto il pianeta, un controllo sui contenuti online, basandosi su *policy rules* e *community guidelines*⁴¹. Per altro verso, nel conflitto tra questo statuto digitale speciale, ma vigente su scala globale, e gli ordinamenti giuridici nazionali, è tuttora controverso quale disciplina debba prevalere⁴².

A causa dell’enorme pressione, del mutamento quotidiano della massa di contenuti digitali⁴³ e della minaccia di sanzioni di una certa entità, previste dal NetzDG, i fornitori di servizi informatici diventano censori contro la loro volontà. “Poiché l’illiceità dei contenuti di norma non è facilmente accertabile né è manifesta, ai fornitori di servizi informatici, in ultima istanza, non resta che la – pressoché incontrollata – rimozione dei contenuti medesimi”⁴⁴. Il NetzDG costituisce sinora un incentivo ad agire in tal senso. Il timore è che, in caso di dubbio, vengano eliminati anche i contenuti leciti (c.d. “*overblocking*”)⁴⁵. Il cittadino internauta è per ora impotente di fronte a questo effetto censorio collaterale, dal momento che il NetzDG ancora non prevede un divieto di cancellazione di contenuti leciti. L’Autorità federale per la giustizia (*Bundesamt für Justiz*, BfJ) accerta solo che i fornitori di servizi informatici abbiano cancellato un contenuto illecito o lo abbiano cancellato in tempo, ma non verifica se il contenuto sia stato correttamente classificato come illecito. La facoltà di eliminare dei contenuti informativi, attraverso la loro cancellazione da un canale comunicativo pubblico, colloca i fornitori di servizi informatici in una posizione di concreta superiorità rispetto ai comuni cittadini internauti, nella quale s’intravede “una novella forma dell’inquisizione risalente alle prime fasi dell’epoca moderna”⁴⁶.

Ma i *service provider* sono sottoposti anche a pressioni da parte degli autori, cioè dei fornitori di contenuti: il ripristino dei contenuti cancellati (procedura “*put-back*”) è

⁴¹ Le *policy rules* sono indipendenti dal diritto penale e possono andare oltre il diritto penale. Si vedano, ad esempio, le *policy rules* di Twitter sul comportamento alimentato dall’odio, inserite nei termini d’uso del servizio (TOS).

⁴² MÜLLER-FRANKEN, *Netzwerkdurchsetzungsgesetz*, cit., p. 9.

⁴³ Solo su *YouTube*, ogni minuto vengono caricate oltre 400 ore di contenuti video.

⁴⁴ Dichiarazione di Google al Ministero federale della giustizia e della tutela dei consumatori sul progetto di legge per il miglioramento dell’applicazione della legge nei social network (NetzDG-E), p. 13, disponibile sul sito

https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2017/Downloads/03302017_Stellungnahme_google_youtube_RefE_NetzDG.pdf?blob=publicationFile&v=2 (Ultimo accesso: 10 febbraio 2021).

⁴⁵ SCHIFF, *Meinungsfreiheit in mediatisierten digitalen Räumen – Das NetzDG auf dem Prüfstand des Verfassungsrechts*, in *MMR* 6/2018, p. 369; v. anche CEFFINATO, *Zur Regulierung des Internet durch Strafrecht*, in *ZStW*, cit., p. 559. Schünemann, dal suo canto, vede giustamente la libertà di espressione in grave pericolo a causa di un *eccesso di blocco*: v. SCHÜNEMANN, *Gefährden Fake News die Demokratie*, cit., p. 629.

⁴⁶ SCHÜNEMANN, *Gefährden Fake News die Demokratie*, cit., p. 626.

stato già oggetto di diverse pronunce in sede civile⁴⁷. L'utente si accolla il rischio iniziale legato alle spese del processo civile⁴⁸, ma i provider sono a loro volta esposti al rischio di incorrere in responsabilità e di risarcire i danni.

III. COMPATIBILITÀ CON I DIRITTI FONDAMENTALI E UMANI.

Con l'entrata in vigore del NetzDG, vengono presi di mira, contemporaneamente, più diritti umani, appartenenti a vari attori dello spazio digitale. I cittadini internauti sono costretti a temere per la loro libertà di opinione, informazione ed espressione artistica, quando i fornitori di servizi informatici bloccano i loro siti web a livello locale o li cancellano a livello globale⁴⁹. Il che, nella maggior parte dei casi e per la maggior parte delle fattispecie, avviene senza aver prima ascoltato gli autori del *post* cancellato o il titolare dell'*account* bloccato, e senza aver messo a loro disposizione rimedi giuridici adeguati. Inoltre, ai provider vengono concesse numerose ingerenze nel diritto all'autodeterminazione informativa, attraverso obblighi di cancellazione, di archiviazione e a breve, se sarà necessario, anche di trasmissione di dati. Tali obblighi non incidono solo sulla posizione degli autori dei contenuti. Chi muove un reclamo nei confronti di un contenuto (senza necessariamente essere la persona offesa dallo stesso) deve anche temere per i suoi diritti personali e per la sua *privacy*, oltre che per il diritto di ottenere giustizia. I fornitori di servizi, a loro volta, devono preoccuparsi soprattutto per la loro libertà di esercizio della professione.

In ragione dell'elevato numero di diritti fondamentali toccati dal NetzDG e della moltitudine dei rispettivi titolari, in questa sede sarà possibile illustrare solo alcuni profili di maggiore interesse. Una disamina sommaria dovrebbe però bastare a dimostrare quanto sia complesso ponderare i diversi interessi coinvolti nella società digitale.

1. Libertà di espressione.

Nell'ambito della tutela della libertà di espressione, protetta dall'art. 19 del Patto internazionale sui diritti civili e politici (ICCPR)⁵⁰, ricadono le *opinioni*, cioè le esternazioni caratterizzate dall'"elemento della presa di posizione e dall'esprimersi in

⁴⁷ Cfr. ad es. OLG Oldenburg del 1.7.2019, 13 W 16/19.

⁴⁸ MÜLLER-FRANKEN, *Netzwerkdurchsetzungsgesetz*, cit., 13.

⁴⁹ Nella cit. dichiarazione sul NetzDG-E, resa al Ministero federale della giustizia e della tutela dei consumatori (p. 21), Google ha sottolineato che una cancellazione globale dei contenuti è una violazione del principio di territorialità e del principio di sovranità dello Stato ai sensi del diritto internazionale.

⁵⁰ Art. 19, comma 1 e comma 2 ICCPR. "1. Ogni individuo ha diritto a non essere molestato per le proprie opinioni. 2. Ogni individuo ha il diritto alla libertà di espressione; tale diritto comprende la libertà di cercare, ricevere e diffondere informazioni e idee di ogni genere, senza riguardo a frontiere, oralmente, per iscritto, attraverso la stampa, in forma artistica o attraverso qualsiasi altro mezzo di sua scelta."

favore di qualcosa"⁵¹. Non importa se tali esternazioni "si rivelano vere o false, se sono giustificate o infondate, emotive o razionali, valide o prive di valore, pericolose o innocue"⁵². Affermazioni corrosive, esagerate, polemiche, offensive e dannose⁵³ rientrano nel concetto di opinione, e quindi nell'ambito di tutela della libertà di espressione, così come le affermazioni colme d'odio, istigatorie e razziste ("*hate speech*"). Inoltre, le *dichiarazioni di fatto* rientrano nel perimetro della tutela, nella misura in cui possano costituire un presupposto per la formazione di opinioni. Tuttavia, le dichiarazioni di fatto deliberatamente false o dimostrate tali, tra cui le c.d. *fake news*, non rientrano nella tutela, non potendo contribuire alla formazione di un'opinione, quale facoltà garantita dal sistema dei diritti umani⁵⁴. Nel caso di dichiarazioni miste, che contengano componenti fattuali e valutative, onde preservare l'efficace tutela dei diritti umani, la dichiarazione deve "essere considerata nel suo complesso espressione di un'opinione, posto che altrimenti si correrebbe il pericolo di una sostanziale restrizione della libertà di opinione"⁵⁵.

Se i contenuti diffusi in formato digitale dai media tradizionali (stampa e radiodiffusione) vengono classificati come illeciti, cancellati o bloccati, sono gioco forza colpiti anche i diritti fondamentali della libertà di stampa e di radiodiffusione. Lo stesso vale per la cancellazione o il blocco di dichiarazioni o immagini artistiche, come misure invasive della libertà di espressione artistica.

Tuttavia, i diritti umani sanciti dall'art. 19, commi 1 e 2 ICCPR non sono garantiti in modo incondizionato. Secondo il terzo comma dello stesso articolo, essi sono soggetti a determinate limitazioni, previste dalla legge, necessarie per il rispetto dei diritti o della reputazione altrui o per la tutela della sicurezza nazionale, dell'ordine pubblico, della salute o della morale pubbliche⁵⁶. L'emanazione di una legge non è sufficiente ad integrare il requisito della previsione legislativa previsto dall'art. 19, comma 3 ICCPR: le restrizioni poste alla libertà di opinione devono essere anche sufficientemente chiare e prevedibili. Inoltre, il requisito della "necessità" implica un giudizio di proporzionalità di siffatte restrizioni, al fine di garantire che esse siano dirette ad un obiettivo specifico e non ledano irragionevolmente i diritti delle persone interessate. La conseguente ingerenza nei diritti di terzi deve essere limitata e giustificata alla luce dell'interesse che tale ingerenza mira a proteggere. Infine, le restrizioni devono essere lo strumento meno invasivo tra quelli astrattamente idonei a conseguire il risultato auspicato.

Il NetzDG è, senza dubbio, una "legge" ai sensi dell'art. 19, comma 3 ICCPR. Tuttavia, la limitazione della libertà di espressione dei cittadini internauti che da essa consegue non è sufficientemente chiara né prevedibile. Lo Stato delega ai provider il potere di decidere sull'applicazione di misure censorie, creando perciò una torre di

⁵¹ BVerfG v. 27 agosto 2019 - 1 BvR 811/17.

⁵² BVerfG v. 27 agosto 2019 - 1 BvR 811/17.

⁵³ MÜLLER-FRANKEN, *Netzwerkdurchsetzungsgesetz*, cit., p. 2.

⁵⁴ BVerfG v. 27 agosto 2019 - 1 BvR 811/17.

⁵⁵ BVerfG v. 27 agosto 2019 - 1 BvR 811/17.

⁵⁶ Art. 19, comma 3 ICCPR.

guardia, privata, sulle opinioni⁵⁷. Dei privati si vedono obbligati a decidere, sotto la minaccia di pesanti sanzioni ed entro un breve termine, se un contenuto *online* corrisponda o meno a uno dei reati elencati dall'art. 1, comma 3 NetzDG, e di conseguenza se cancellarlo o bloccarlo. Entro tempi di reazione assai rapidi, essi devono "effettuare un bilanciamento tra contenuti controversi e tutela della libertà di espressione"⁵⁸, senza previa audizione dell'utente ed in mancanza di un controllo giudiziario. In tal modo, i fornitori di servizi informatici sono indotti ad assolvere una funzione di giustizia parallela di tipo privato. Si è al cospetto di una concreta minaccia per la libertà di espressione, di informazione e di espressione artistica.

Il problema dell'impiego di soggetti privati come sentinelle delle opinioni espresse in pubblico è acuito dal fatto che gli strumenti a disposizione dei provider, ai sensi del § 1, comma 3 NetzDG, lasciano molto a desiderare dal punto di vista della determinatezza. Numerose pronunce, aventi ad oggetto molte delle fattispecie comprese nel catalogo normativo di cui al NetzDG, dimostrano che delineare in via interpretativa i confini tra queste fattispecie e la libertà di opinione è operazione estremamente controversa. La prassi dimostra come espressioni normalmente ritenute volgari siano state in parte giudicate "per un pelo entro il limite di ciò che è ancora accettabile per gli interessati", e quindi ancora coperte dalla libertà di espressione⁵⁹. Anche rispetto al § 130 StGB, alcune Procure sono state costrette ad avviare le indagini solo a seguito di una richiesta del Tribunale. Il che dimostra come neppure per l'autorità giudiziaria sia facile discernere i contenuti illeciti sui social network. Tanto più inopportuno appare delegare questo compito a soggetti privati.

2. Diritto allo sviluppo della personalità, in generale, e diritto all'autodeterminazione informativa, in particolare.

Se una persona lesa possa rivendicare una tutela contro la denigrazione subita attraverso un post in un social network, disponendo con ciò della rappresentazione della propria persona in pubblico, è questione connessa alla protezione, assicurata anche in diritto civile, del diritto generale allo sviluppo della personalità di cui all'art. 2, comma 1 (in combinato disposto con l'art. 1, comma 1) della Costituzione federale tedesca (*Grundgesetz*, GG). Questo diritto è diametralmente opposto alla libertà di espressione degli autori dei contenuti in rete, con il quale deve essere bilanciato.

Ma il trattamento dei dati personali richiesto dal NetzDG incide in vario modo anche sulla peculiare conformazione del diritto all'autodeterminazione informativa.

⁵⁷ MÜLLER-FRANKEN, *Netzwerkdurchsetzungsgesetz*, cit., p. 7.

⁵⁸ Dichiarazione di Google Ireland Ltd. al Ministero Federale della Giustizia e della Tutela dei Consumatori sulla proposta di legge per combattere l'estremismo di destra e i crimini motivati dall'odio, p. 2, disponibile sul sito

https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2020/Downloads/011720_Stellungnahme_google_RefE_Belaempfung-Rechtsextremismus-Hasskriminalitaet.pdf?__blob=publicationFile&v=3 (Ultimo accesso: 10 febbraio 2021).

⁵⁹ Decisione dell'LG Berlin del 09.09.2019 - 27 AR 17/19.

Con il NetzDG il legislatore delega i provider ad effettuare numerose incursioni nel diritto all'autodeterminazione informativa, richiedendo altresì l'archiviazione per settimane dei dati personali degli autori dei contenuti ed eventualmente anche dei denunciati e dei trasgressori. Né i contributi scritti o consistenti in immagini, né i relativi dati degli utenti e di traffico possono essere rimossi (o consensualmente conservati) a discrezione delle parti coinvolte. Il NetzDG specifica piuttosto quali dati, dove e come debbano essere memorizzati o cancellati. E ciò vale anche per le modifiche in cantiere del NetzDG e per gli obblighi di comunicazione e trasmissione che esse implicheranno⁶⁰.

Anche in ragione dei notevoli margini interpretativi, che come detto caratterizzano la valutazione dei contenuti, si determina una situazione di incertezza per tutte le parti coinvolte, con erosione dei confini della sfera privata.

Nella sentenza sul censimento (*Volkszählungsurteil*)⁶¹, la Corte costituzionale federale ha formulato un assunto cruciale in merito al diritto alla tutela dei dati (sancito dagli artt. 1, comma 1 e 2, comma 1 GG), contribuendo, al tempo stesso, in maniera rilevante allo sviluppo della disciplina della protezione dei dati personali: "Un ordine sociale e un ordinamento giuridico che lo renda possibile, nei quali i cittadini non possano sapere chi sa qualcosa su di loro, che cosa, quando ed in quale occasione, non sarebbero compatibili con il diritto all'autodeterminazione informativa. Chi teme che i comportamenti alternativi possano essere notati in qualsiasi momento e costantemente memorizzati, utilizzati o trasmessi come informazione, proverà a non esporsi attraverso simili comportamenti. [...] Il che comprometterebbe non solo le possibilità di sviluppo dell'individuo, ma anche il bene comune, perché l'autodeterminazione è una condizione elementare per il funzionamento di una comunità democratica libera, basata sulla capacità dei suoi cittadini di agire e partecipare"⁶².

L'incertezza descritta nella sentenza della Corte costituzionale federale non riguarda solo gli autori dei contenuti, che sono sempre meno in grado di osservare la lunga e duratura scia di dati gettata da un "posting". Le persone lese e quanti siano intenzionati a muovere un reclamo potrebbero – in futuro, ma già ora – rifuggire dal contatto con i social network, se non potranno più essere sicuri del fatto che i loro dati personali rimarranno tra privati e non dovranno essere immagazzinati per consentirne l'accesso allo Stato o addirittura, in futuro, allo Stato anticipatamente rivelati.

3. Libertà della professione.

Il diritto fondamentale alla libertà della professione, sancito dall'articolo 12 GG, garantisce a ciascuno la libertà di scegliere la propria occupazione e il proprio posto di

⁶⁰ Su questo possibile – e molto invasivo – sviluppo si tornerà *infra* par. VI.

⁶¹ BVerfG, sentenza del primo Senato del 15 dicembre 1983 - 1 BvR 209/83.

⁶² BVerfG, sentenza del primo Senato del 15 dicembre 1983 - 1 BvR 209/83, comma 146.

lavoro, nonché la libertà di esercitare la propria professione⁶³. L'ambito di tutela abbraccia l'intera attività professionale, compresa la scelta della forma in cui questa è concretamente esercitata. Titolari del diritto sono le persone fisiche e, ai sensi dell'articolo 19, comma 3 GG anche le persone giuridiche (nazionali ed europee)⁶⁴, nella misura in cui esercitano "un'attività con fine di lucro che, per sua natura e conformazione, è egualmente accessibile a una persona giuridica come ad una persona fisica"⁶⁵. I fornitori di servizi informatici rientrano quindi nell'ambito della tutela della libertà di professione.

Neanche la libertà di professione è priva di limiti. Ai sensi dell'articolo 12, comma 1, secondo periodo GG, *l'esercizio di una professione* può essere limitato in base alla legge e nel rispetto del principio di proporzionalità⁶⁶. Il § 3, comma 2 NetzDG obbliga i fornitori a cancellare o a bloccare entro determinati limiti di tempo i contenuti "manifestamente" illeciti e quelli senza altra specificazione "illeciti". Quest'obbligo interferisce con la libertà professionale dei fornitori di servizi informatici, nella misura in cui incide sulla disciplina della loro attività professionale.

Secondo la giurisprudenza consolidata della Corte costituzionale federale, presupposti della legittimità costituzionale di un intervento di questo tipo sono il perseguimento di uno *scopo legittimo* ed il rispetto del *principio di proporzionalità*.⁶⁷ Scopi del NetzDG sono la prevenzione dei rischi per la pubblica sicurezza e la promozione di un cambiamento nella cultura del dibattito in nome della lotta ai crimini d'odio e alle *fake news* nei social network. Sulla legittimità di tali scopi non possono sorgere dubbi.

Tuttavia, occorre chiedersi se il NetzDG sia anche un mezzo proporzionato al raggiungimento dei suoi (legittimi) scopi, se cioè sia adeguato, necessario e proporzionato in senso stretto. "Una regolamentazione giuridica è costituzionalmente *idonea*, già solo se l'obiettivo auspicato può essere promosso mediante il suo supporto, sì che è sufficiente la possibilità di raggiungere lo scopo"⁶⁸. In tal senso, la cancellazione immediata (o il blocco) di contenuti manifestamente o *sic et simpliciter* illeciti, ai sensi dell'art. 3, comma 2 NetzDG è idonea ad eliminare disturbi alla sicurezza pubblica e a modificare la cultura del dibattito per combattere i crimini d'odio e le *fake news*.

Ma la limitazione della libertà professionale dei provider deve essere anche *necessaria*. Una limitazione è sempre necessaria, se non c'è un altro mezzo idoneo, più

⁶³ GRÖPL, *Art. 12*, Rdnr. 15, in Gröpl, Windthorst, Coelln (Hrsg.), *StuKo GG*, 4° ed. 2020.

⁶⁴ Cfr., per l'estensione del diritto fondamentale alle persone giuridiche degli Stati membri dell'Unione Europea, BVerfGE 129, 78 (94 ss.).

⁶⁵ Giurisprudenza costante della Corte costituzionale federale: cfr. BVerfGE 50, 290 (363); BVerfGE 105, 252 (265).

⁶⁶ Giurisprudenza costante della Corte costituzionale federale: cfr. solo BVerfGE 135, 90 (111), con ulteriori riferimenti.

⁶⁷ LADEUR, GOSTOMZYK, *Gutachten zur Verfassungsmäßigkeit des Entwurfs eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz -NetzDG) i.d.F. vom 16. Mai 2017 - BT-Drs. 18/12356 - Erstattet auf Ansuchen des bitkom*, 2017, p. 33, disponibile sul sito <https://www.bitkom.org/sites/default/files/file/import/NetzDG-Gutachten-Gostomzyk-Ladeur.pdf> (ultimo accesso: 10 febbraio 2021).

⁶⁸ Giurisprudenza costante della Corte costituzionale federale, cfr. BVerfGE 126, 112 (144).

mite, in grado di conseguire l'obiettivo con pari o simile efficacia⁶⁹. Quale mezzo più mite, nel nostro caso, potrebbe concepirsi un irrigidimento delle regole sociali della comunicazione (*policy rules*), stabilite dai provider stessi; inoltre, si potrebbe prospettare una combinazione di autoregolamentazione e controllo delle condotte in forma di "strategia cooperativa pubblico-privata"⁷⁰, attuabile mediante provvedimenti di vigilanza ed in grado di garantire più ampi margini di manovra ai provider.

Il NetzDG non dovrebbe andare oltre quanto è necessario per il perseguimento dei suoi scopi, né eccedere gli scopi stessi⁷¹. Tuttavia, l'imposizione legislativa di obblighi di cancellazione e di blocco dei contenuti entro un breve termine dalla presentazione di un reclamo o dalla conoscenza del contenuto contestato, con le relative conseguenze sanzionatorie, conduce in molti casi alla rimozione (o al blocco) di contenuti leciti, dovuta all'assenza di una chiara definizione legale, comportando quindi notevoli danni collaterali⁷². Ogni caso dubbio volge presumibilmente a scapito della libertà di comunicazione⁷³. Per tanto, gli obblighi di cui al § 3, comma 2 NetzDG vanno al di là di quanto è necessario al perseguimento degli obiettivi legislativi.

Infine, la disposizione di cui all'art. 3, comma 2 NetzDG è anche *sproporzionata in senso stretto*, in quanto impone un pesante onere ai fornitori di servizi informatici, soggetto a sanzione pecuniaria, senza distinguere in base alla gravità della lesione. Diviene lecito chiedersi se "anche affermazioni di esigua gravità, lette da pochissimi, debbano essere cancellate e perseguite con ingente sforzo [...]"⁷⁴. La legge, insomma, non lascia tempo né spazio per un bilanciamento tra beni.

Il NetzDG interferisce così in modo sproporzionato con la libertà professionale dei fornitori di servizi informatici. La pressione esercitata nei loro confronti attraverso la minaccia di sanzioni legali, non solo viola la loro libertà professionale, ma li induce anche, indirettamente, a violare il diritto fondamentale alla libertà di espressione degli utenti, ossia dei loro clienti, attraverso giudizi sommari sulla liceità delle opinioni manifestate da costoro⁷⁵.

⁶⁹ BVerfGE 80, 1 (30).

⁷⁰ Vedi LADEUR, GOSTOMZYK, *Gutachten zur Verfassungsmäßigkeit*, cit., p. 58.

⁷¹ Cfr. BVerfGE 79, 179 (198); BVerfGE 100, 226 (241); BVerfGE 110, 1 (28).

⁷² La bozza del NetzDG prevedeva inizialmente danni collaterali ancora maggiori: i fornitori di servizi IT dovevano essere obbligati - oltre alla cancellazione di contenuti discutibili - a cancellare anche tutte le "copie". Per questo si sarebbero dovuti utilizzare potenti filtri e quindi potenti macchine di censura, che avrebbero eliminato tutti i contenuti identici senza considerare il rispettivo contesto. Si veda la dichiarazione di Google al Ministero federale della giustizia e della tutela dei consumatori, cit., 22.

⁷³ Dichiarazione di Google al Ministero federale della giustizia e della tutela dei consumatori, cit., p. 14.

⁷⁴ LADEUR, GOSTOMZYK, *Gutachten zur Verfassungsmäßigkeit*, cit., p. 60 s.

⁷⁵ LADEUR, GOSTOMZYK, *Gutachten zur Verfassungsmäßigkeit*, cit., p. 80.

IV. LEGGE PER COMBATTERE L'ESTREMISMO DI DESTRA E I CRIMINI D'ODIO.

1. Obiettivo.

Il progetto di "Legge per combattere l'estremismo di destra e i crimini d'odio" (GBRH-E) del 18 febbraio 2020, approvato dal *Bundestag* tedesco il 18 giugno e dal *Bundesrat* il 3 luglio 2020, rappresenta un ulteriore stadio nella strategia di lotta all'odio, all'istigazione criminosa e alla diffusione di contenuti illeciti in internet, caratterizzato soprattutto dalla previsione di ulteriori obblighi imposti ai fornitori di servizi informatici. La legge intende favorire una più intensa ed efficace persecuzione di tali fenomeni, sì da tutelare la quiete pubblica ed il libero svolgimento del discorso politico quale fondamento di una società democratica.

Nell'ottobre 2020, il Presidente della Repubblica federale ha sospeso la procedura di approvazione di questa legge, esprimendo dubbi sulla sua costituzionalità⁷⁶. Secondo il Presidente, la legge conterrebbe delle disposizioni in contrasto con i principi riconosciuti dalla Corte costituzionale federale in una pronuncia del 17 luglio 2020 (quindi pubblicata dopo l'approvazione del GBRH-E da parte del *Bundesrat*) in materia di telecomunicazioni. Al momento, il Governo federale sta apportando delle modifiche al testo, con l'intenzione di presentarle a breve al *Bundestag*.

2. Contenuto essenziale.

La legge prevede un inasprimento delle disposizioni del Codice penale (StGB-E), del Codice di procedura penale (StPO-E), della legge federale sulla registrazione dei cittadini (BMG-E), della legge sull'Ufficio federale di polizia giudiziaria (BKAG-E), della legge sui media telematici (TMG-E) e infine del NetzDG (NetzDG-E). Per esigenze di sintesi, sono di seguito illustrate in modo più dettagliato solo le modifiche al codice penale e al NetzDG.

a) Modifiche al codice penale

Il diritto penale subisce un notevole inasprimento per effetto dalla Legge per combattere l'estremismo di destra e i crimini d'odio, soprattutto mediante un ampliamento del catalogo dei reati e l'estensione della punibilità ad atti prodromici all'effettiva lesione di un bene giuridico.

Anzitutto, la legge estende la fattispecie di minaccia contenuta nel § 241 StGB. Finora, chi minacciava una persona di commettere un *crimine* (*Verbrechen*) contro di lei o contro una persona a lei vicina, era punito con la reclusione fino a un anno o con una multa. In futuro, saranno punibili anche minacce di realizzare fatti contro

⁷⁶ Si veda Deutscher Bundestag, Drucksache 19/23867, vom 2.11.2020, in <https://dipbt.bundestag.de/dip21/btd/19/238/1923867.pdf> (Ultimo accesso: 10 febbraio 2021).

l'autodeterminazione sessuale, l'integrità fisica, la libertà personale o contro cose di valore significativo; di conseguenza, diverrà punibile anche la minaccia di commettere un *delitto (Vergehen)* contro il destinatario o una persona a lui vicina. La cornice edittale sarà elevata fino a due anni, per la minaccia in rete, e fino a tre anni di reclusione in alternativa alla multa per la minaccia, effettuata in pubblico, di commettere un crimine⁷⁷.

Vengono poi aumentate le pene per l'ingiuria ai sensi dell'art. 185 StGB. Chiunque insulti pubblicamente gli altri in internet potrà, in futuro, essere punito con la reclusione fino a due anni, invece di un anno come in precedenza. Il reato di diffamazione e menzogna diffamatoria contro personaggi della vita politica, previsto dal § 188 StGB, si applicherà a tutti i livelli politici, e quindi anche ai politici locali, e sarà esteso anche alla protezione contro le ingiurie.

La fattispecie di remunerazione ed apologia di reati, punita dal § 140 StGB, sarà estesa sino a comprendere anche l'approvazione di *futuri* reati gravi, se idonei a turbare la pubblica quiete.

Il catalogo dei reati di disturbo della pubblica quiete e di minaccia di reato ai sensi del § 126 StGB includerà anche la minaccia di danni fisici *pericolosi* ai sensi del § 224 StGB, quindi un *delitto (Vergehen)*, nonché la minaccia di gravi reati contro l'autodeterminazione sessuale.

Il reato di resistenza o di aggressione a persone che svolgono funzioni equiparate a quelle degli ufficiali di polizia, ai sensi del § 115 StGB, sarà esteso al personale del servizio medico di emergenza e del pronto soccorso.

Infine, ai criteri di commisurazione della pena di cui al § 46, comma 2 StGB – ai sensi del quale il giudice bilancia le circostanze favorevoli con quelle sfavorevoli del reo –, viene aggiunto, quale fattore aggravante, l'aver agito con motivazioni antisemite.

b) Modifiche al NetzDG

Il nucleo della legge per la lotta contro l'estremismo di destra e i crimini d'odio è l'introduzione di un obbligo di segnalazione a carico dei gestori di *social network* per *determinati reati*, compresi nel catalogo di cui al § 1, comma 3 NetzDG. È quanto prevede il § 3a del progetto di modifica del NetzDG (di seguito NetzDG-E).

In ottemperanza a tale obbligo di segnalazione, onde consentire il perseguimento di reati, i provider dovranno comunicare all'Ufficio federale di polizia criminale (BKA) quei contenuti oggetto di una denuncia nei loro confronti, che il provider abbia rimosso o dei quali abbia bloccato l'accesso, sempre che vi siano *indizi concreti* che il contenuto in questione sia sussumibile in una fattispecie inclusa nel § 3, comma 2 n. 3a del NetzDG-E e non sia giustificato (§ 3a, comma 2 NetzDG-E). La comunicazione al BKA dovrà contenere il contenuto incriminato e, se disponibile, per consentire una più rapida

⁷⁷ OĞLAKCIOĞLU, "Haters gonna hate ... (and lawmakers hopefully gonna make something else)" - Einige Anmerkungen zum Regierungsentwurf zur Bekämpfung der Hasskriminalität, in ZStW 132, 2020, pp. 535 ss., p. 535 rileva a ragione criticamente: "[w]enn der Strafraumen durch die Ausweitung der Bezugstaten ausgedehnt wird, hat dies [...] zu Folge, dass [...] erstmals die Bedrohung mit einer Straftat strafbar ist, deren Verwirklichung (!) denselben Strafraumen aufweist (bspw. § 184i StGB)".

identificazione degli autori, l'indirizzo IP, compreso il numero di porta che l'utente ha utilizzato nel condividere il contenuto con altri utenti o nel renderlo accessibile al pubblico (§ 3a, comma 4 NetzDG-E).

Il provider informa i suoi clienti della segnalazione 14 giorni dopo la comunicazione alla BKA. Entro i 14 giorni dalla segnalazione, la BKA può ordinare al provider di segretare le informazioni nei confronti dei clienti, in caso di pericolo per le indagini, per la vita, l'integrità fisica o la libertà di una persona o per valori patrimoniali di rilevante entità (§ 3a, comma 6 NetzDG-E). Nel caso in cui emetta tale ordine, la BKA è tenuta ad informare l'utente della segnalazione ricevuta, non appena ciò sia possibile senza pregiudizio per lo scopo dell'indagine (§ 3a, comma 6 NetzDG-E).

L'obbligo di segnalazione comprende la diffusione di materiale di propaganda e l'uso di simboli di organizzazioni anticostituzionali ai sensi dei §§ 86 e 86a StGB, la preparazione di un grave atto di violenza che metta in pericolo lo Stato, ai sensi dei §§ 89a e 91 StGB, la formazione e il sostegno di organizzazioni criminali e terroristiche ai sensi dei §§ 129, 129a e 129b StGB, l'istigazione all'odio e la rappresentazione della violenza ai sensi dei §§ 130, 131 StGB, nonché il disturbo della quiete pubblica mediante minaccia di commettere reati ai sensi del § 126 StGB, la ricompensa e l'apologia di reati ai sensi del § 140 StGB, la minaccia di commettere reati contro la vita, l'autodeterminazione sessuale, l'integrità fisica o la libertà personale, ai sensi del § 241 StGB, e la diffusione di materiale pedopornografico ai sensi del § 184b StGB. Non rientrano nell'obbligo di segnalazione l'ingiuria, la diffamazione e la menzogna diffamatoria. In futuro, tuttavia, i gestori di *social network* dovranno informare gli utenti su come e dove possono sporgere denuncia e, se necessario, una querela.

3. Dubbi di costituzionalità e osservazioni critiche.

Gli obblighi di segnalazione dei fornitori di servizi informatici, connessi agli obblighi di cancellazione e di blocco, rappresentano un ulteriore sviluppo, altamente problematico, del sistema di *compliance* delineato nel NetzDG.

In base all'obbligo di segnalazione, i responsabili devono essere perseguiti in modo mirato. A tal fine, i fornitori di servizi informatici devono stabilire quando sussistono *indizi concreti*, nell'accezione di *Anfangsverdacht* ("sospetto iniziale") tipica del diritto processuale penale, in relazione a determinate fattispecie penali. Questo obbligo proattivo di segnalazione, previsto dalla legge, trasforma i privati in "guardiani del meccanismo di sussunzione [dei contenuti] entro complesse fattispecie penali"⁷⁸. La

⁷⁸ Dichiarazione dell'ordine degli avvocati tedeschi del Comitato di diritto penale sul progetto di legge per la lotta contro il crimine d'odio e l'estremismo di destra (gennaio 2020), p. 4, disponibile sul sito https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2020/Downloads/012820_Stellungnahme_DAV_RefE__Belaempfung-Rechtsextremismus-Hasskriminalitaet.pdf;jsessionid=CE98DC499D8D882830A543AE6E1C40D4.2_cid289?__blob=publicazioneFile&v=3 (ultimo accesso: 10 febbraio 2021).

decisione iniziale su quale contenuto debba essere perseguito è rimessa a dei privati⁷⁹: il che introduce una palese anomalia nel sistema, dal momento che perseguire i reati è prerogativa del potere sovrano. È dunque necessario opporsi ad un simile sviluppo, che tende ad accollare prerogative sovrane ad attori privati. Una possibile soluzione – se si vuole mantenere l’obbligo di segnalazione – potrebbe consistere nell’imporre ai fornitori di servizi informatici, in un primo momento, solo l’obbligo di trasmettere i contenuti presumibilmente illeciti, per poi comunicare all’autorità giudiziaria l’indirizzo IP, compreso il numero di porta, solo dopo che l’autorità abbia constatato la sussistenza di un *Anfangsverdacht*. Fino alla statuizione relativa all’*Anfangsverdacht*, i dati potrebbero essere conservati, e dunque protetti, in una procedura “quick freeze”⁸⁰.

La prevista trasmissione in massa di contenuti, indirizzi IP e password da parte di privati alla BKA genererà un accumulo di dati di entità senza precedenti. Tale adempimento è per di più in contraddizione con l’obbligo dei fornitori di servizi informatici di garantire la sicurezza dei dati, sì che conduce ad un conflitto di doveri⁸¹. La trasmissione dovrebbe avvenire in assenza di sufficienti meccanismi di controllo, ipotizzabili, ad esempio, in caso di un controllo giudiziario. La divulgazione delle password consentirà poi di effettuare facilmente “perquisizioni domiciliari online” da parte dei dipartimenti di polizia. Poco chiare sono anche le modalità di elaborazione, archiviazione e cancellazione di questa massa di dati presso la BKA, ed estremamente problematica è la segretezza – prevista dalla legge – della trasmissione di dati da parte di privati alla BKA⁸².

In sintesi, come affermato da un’importante associazione di categoria, la trasmissione proattiva di “dati personali costituisce un’ingerenza di vasta portata nel

⁷⁹ Dichiarazione di bitkom del 17 gennaio 2020 sul progetto di legge per combattere i crimini motivati dall’odio e l’estremismo di destra p. 8, disponibile su https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2020/Downloads/011720_Stellungnahme_Bitkom_RefE__Belaempfung-Rechtsextremismus-Hasskriminalitaet.pdf;jsessionid=CE98DC499D8D882830A543AE6E1C40D4.2_cid289?__blob=publicationFile&v=3 (ultimo accesso: 10 febbraio 2021).

⁸⁰ Su questa proposta si veda il parere dell’Incaricato federale per la protezione dei dati e la libertà d’informazione sul progetto di legge contro l’estremismo di destra e i crimini motivati dall’odio del 26 febbraio 2020, p. 3, disponibile sul sito https://www.bfdi.bund.de/DE/Infothek/Transparenz/Stellungnahmen/2020/Stellungnahme_Gesetz_Bek%C3%A4mpfung_Hasskriminalit%C3%A4t.pdf;jsessionid=80E51BC903825D17AB96CAFB97E69703.1_cid329?__blob=publicationFile&v=1 (ultimo accesso: 8 marzo 2021).

⁸¹ Dichiarazione di Google Ireland Ltd. al Ministero Federale della Giustizia e della Tutela dei Consumatori sulla proposta di legge per combattere l’estremismo di destra e i crimini motivati dall’odio, cit., p. 3.

⁸² Dichiarazione dell’Associazione dell’industria di Internet (*Verband der Internetwirtschaft e.V.*) del 17 gennaio 2020 sul disegno di legge per la lotta all’estremismo di destra e ai crimini motivati dall’odio, p. 4, disponibile sul sito https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2020/Downloads/011720_Stellungnahme_eco_RefE__Belaempfung-Rechtsextremismus-Hasskriminalitaet.pdf;jsessionid=CE98DC499D8D882830A543AE6E1C40D4.2_cid289?__blob=publicationFile&v=3 (ultimo accesso: 10 febbraio 2021)

diritto fondamentale alla protezione dei dati e nel diritto fondamentale all'autodeterminazione informativa"⁸³.

V. Conclusioni.

Internet, come piattaforma di comunicazione globale, offre a ciascuno un'opportunità unica di "connettersi ovunque ed istantaneamente con miliardi di persone da tutto il mondo"⁸⁴, richiamando su di sé l'attenzione. La stragrande maggioranza delle persone usa internet per scopi legittimi, ma ci sono anche dichiarazioni lesive dei diritti umani da parte di gruppi ed individui che diffondono odio, minacce, contenuti violenti, efferati, dannosi o pericolosi, allusioni violente o notizie false. I tweet di Donald Trump, che diffondevano disinformazione, *fake news* o notizie "alternative", aizzando ed istigando all'odio, ne sono soltanto un esempio notorio.

Nondimeno, lo spazio digitale non è uno spazio libero dal diritto o nel quale la pena risulti inapplicabile⁸⁵. I contenuti illeciti devono essere contrastati con decisione, ma anche in modo adeguato. Già prima dell'entrata in vigore del NetzDG, i fornitori di servizi informatici erano obbligati, in qualità di *host provider*, a rimuovere i contenuti illeciti non appena ne fossero venuti a conoscenza, vale a dire senza colpevole ritardo⁸⁶. Adesso il NetzDG affida in buona parte ai privati il compito di far rispettare la legge. Così facendo, lo Stato di diritto si sottrae alle proprie responsabilità e mette in conto massicce restrizioni alla libertà di comunicazione ed alla libertà professionale. "Eppure, proprio là dove la linea di demarcazione tra espressioni consentite e vietate non è chiara, e s'impone un'attenta ponderazione degli interessi costituzionali, la valutazione giuridica non dovrebbe essere compiuta da imprese private, ma essere riservata ai giudici [e con ciò allo Stato di diritto]⁸⁷". All'"*overblocking*" del NetzDG si aggiunge il pericolo di "*overreporting*", che va anche a scapito della libertà di espressione.

Il NetzDG trasforma i *social network*, contro il loro volere, in sentinelle private della pubblica opinione. In futuro, inoltre, nel contesto del NetzDG – come già avvenuto nel settore della sorveglianza delle telecomunicazioni –, essi fungeranno da ausiliari delle forze dell'ordine. I clienti saranno incerti tra l'essere ancora e solo parte di un normale rapporto di utenza con il fornitore di servizi informatici, oppure già indagati nell'ambito di un procedimento obbligatoriamente attivato per iniziativa di quest'ultimo. Con l'eventuale eccezione dei reati procedibili a querela, alla lunga anche le persone offese potrebbero essere inconsapevoli del fatto che i loro dati sono oggetto

⁸³ Dichiarazione di bitkom, cit., p. 10.

⁸⁴ Si veda la dichiarazione di Google al Ministero federale della giustizia e della tutela dei consumatori, cit., p. 5.

⁸⁵ Per quanto riguarda l'applicazione della legge su Internet, si veda SIEBER, *Straftaten und Strafverfolgung im Internet*. Sonderdruck aus: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen des 69. Deutschen Juristentages, Band 1 – Gutachten, München 2012, pp. C1–157.

⁸⁶ Cfr. art. 14 della direttiva sul commercio elettronico 2000/31/CE e §10 TMG.

⁸⁷ Dichiarazione di Google al Ministero federale della giustizia e della tutela dei consumatori, cit., p. 14.

di una memorizzazione a lungo termine, o addirittura sono già trasmigrati nella fase di indagini di un procedimento penale⁸⁸.

Come visto in relazione al diritto all'autodeterminazione informativa, richiamando la sentenza della Corte costituzionale sul censimento, è proprio questa incertezza ad avere conseguenze negative per il bene comune.⁸⁹ Contenimento ed intimidazione sono effetti prospettabili non solo dal punto di vista della protezione dei dati⁹⁰; nella prospettiva della libertà di opinione, un analogo *chilling effect*, in forma di deferente autocensura preventiva, è un pericolo noto per una società democratica. Da questo punto di vista, le scelte effettuate dal legislatore tedesco per contrastare i contenuti illeciti nello spazio digitale paiono alquanto discutibili.

⁸⁸ Lo si rileva, giustamente, nella relazione di Google Ireland Ltd al Ministero federale della giustizia e della tutela dei consumatori sulla proposta di legge contro l'estremismo di destra e i crimini motivati dall'odio, cit., p. 29.

⁸⁹ Supra § III. 2.

⁹⁰ Sul diritto penale della protezione dei dati personali, fondamentale NOLDE, *Datenschutzstrafrecht*, in: Böttger (Hrsg.), *Wirtschaftsstrafrecht in der Praxis*, 2. Aufl. 2015, pp. 1112–1173.