V.3.3 Politics I: Zensurinfrastruktur und Privatisierung der Rechtsdurchsetzung?

Ein breites Spektrum zivilgesellschaftlicher und wirtschaftlicher Akteure reagierte auf die Verabschiedung des NetzDG mit einer »Deklaration für die Meinungsfreiheit« (Digitale Gesellschaft 2017) und brachte insbesondere drei Argumente gegen die konkrete Umsetzung in Stellung:

1. *Privatisierung der Rechtsdurchsetzung*: Das NetzDG überträgt »staatliche Aufgaben der Rechtsdurchsetzung an Privatunternehmen«.
2. *Einschränkung der Meinungsfreiheit*: Hohe Bußgelder und kurze Löschfristen verstärken »die Gefahr, dass sich Plattformbetreiber im Zweifel zu Lasten der Meinungsfreiheit und für die Löschung oder Sperrung solcher Inhalte entscheiden«.
3. *Privatisierung der Rechtsetzung*: »Die Prüfung der Strafbarkeit oder Rechtswidrigkeit eines Inhalts […] muss auch weiterhin von Gerichten übernommen werden.«

Diese drei Aspekte stehen in den beiden folgenden Unterkapitel sowie in Kapitel V.3.5 noch einmal explizit im Fokus.

V.3.3.1 Kooperation bei oder Privatisierung der Rechtsdurchsetzung?

Eine Übertragung hoheitlicher Aufgaben auf privatwirtschaftliche Akteure – Unternehmen und Konzerne – findet nicht erst im digitalen Zeitalter statt. Sie ist vielmehr Kennzeichen des Übergangs vom intervenierenden Leistungs- zum kooperierenden Gewährleistungsstaat (siehe Kapitel IV.3.2). Dabei steht gerade die Einbeziehung monopolartiger Organisationen in (pfadabhängiger) Tradition korporatistischer Arrangements zwischen Staat und Verbänden. Denn die relevante Größe und Stellung der einbezogenen Organisationen stellt einen zentralen Grund für die dabei erwarteten (wechselseitigen) Vorteile (wie die Entlastung des Staates) sowie die Legitimität der Einbeziehung dar (siehe Kapitel III.1.4).

Eine Kombination aus Selbst- und Ko-Regulierung ist auch im Bereich der Medien alles andere als neu. Sie findet etwa als verbandliche Selbstregulierung bereits seit Jahrzehnten statt. Seit 1948 besteht die Freiwillige Selbstkontrolle der Filmwirtschaft (FSK) zur Alterseinstufung von Filmen, seit 1994 die Unterhaltungssoftware Selbstkontrolle (USK) für Spiele und Software sowie die Freiwillige Selbstkontrolle Fernsehen (FSF) zur Prüfung von Sendungen vor Ausstrahlung, etwa auf Gewalt. Analog dazu wurde 1997 die Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM) zum Umgang mit Internetinhalten insbesondere in Bezug auf den Jugendschutz geschaffen.

Aufbauend auf diesen Erfahrungen gründeten Unternehmen der IKT-Branche 2011 den Verein Selbstregulierung Informationswirtschaft (SRIW) »als unabhängige, **private Aufsichtsstelle branchenspezifischer Verhaltensregeln** [Herv. i. O.]«, um »die notwendigen, **unabhängigen Strukturen** bereitzustellen, um branchenspezifische Verhaltensregeln sowohl **zu verwalten** als auch **glaubwürdig und wirksam zu beaufsichtigen** [Herv. i. O.]« (SRIW o.J.). Aufgabe und Ziel des SRIW (ebd.) ist es, »durch **glaubwürdige und wirkungsvolle Selbst- und Ko-Regulierung**, vor allem **im Bereich des Daten- und**

Verbraucherschutzes, eine innovationsfreundliche und moderne Politikgestaltung zu etablieren [Herv. i. O.].«

Bezogen auf die aktive Rolle der Plattformen im NetzDG, warnten unterschiedliche Akteure in ihren Stellungnahmen jedoch wiederholt vor den Gefahren einer solchen Einbindung, die als Privatisierung der Rechtsdurchsetzung sowie Privatisierung der Rechtsetzung (dazu später ausführlich in Kapitel V.3.5) charakterisiert wurde. »Staatliche Aufgaben der Rechtsdurchsetzung wurden so mit dem NetzDG an Privatunternehmen übertragen. Der Rechtsweg wird so ausgehebelt« (Digitale Gesellschaft 2018). Und sogar der SRIW (2017: 5) stellt fest, dass »das Gewaltmonopol des Staates zumindest in Ansätzen in den privaten Bereich verlagert wird«.

Ein Unterschied zu den eingangs erwähnen korporatistischen Arrangements besteht darin, dass hier nicht primär verbandliche Kollektivorganisationen eingebunden werden, sondern direkt die großen Plattformen und damit globalen Internetkonzerne. Der entscheidende Kritikpunkt liegt jedoch in den übertragenen Aufgaben:

> »Vom Anbieter eines sozialen Netzwerks verlangt der Entwurf, dass dieser über die Strafbarkeit derselben Handlungen innerhalb starrer und sehr kurzer Fristen nicht nur entscheidet, sondern die betreffenden Inhalte auch (endgültig) entfernt« (DGRI 2017: 8).

Die privaten Internetkonzerne entscheiden damit nicht nur anstelle von Gerichten über die Rechtswidrigkeit von Inhalten. Zugleich legen sie für die Akzeptanz von Inhalten zusätzlich ganz eigene Regeln, etwa in Community-Richtlinien, an (siehe Kapitel V.3.5 zur Privatisierung der Rechtsetzung). Darüber hinaus sah das NetzDG auch keine Widerspruchsverfahren gegen (unberechtigtes) Entfernen oder Sperren vor. Nicht zuletzt können Plattformen automatisierte Verfahren zur Entscheidungsfindung einsetzen. In diesem Fall findet eine Regulierung durch Algorithmen [Governance *by* Algorithms] oder algorithmische Steuerung von privater Seite statt. Da diese neue Form der Steuerung auch von staatlicher Seite eingesetzt werden kann, wird sie in Kapitel VI.1.1.2 vertiefend behandelt. Im Gegensatz zu der etablierten Form – Privatisierung und Liberalisierung durch die Etablierung von Aufsichtsbehörden und Regulierungsagenturen zu flankieren – stellt sich hier die Frage, wie eine Regulierung von Algorithmen [Governance *of* Algorithms] am effektivsten implementiert werden kann (siehe Kapitel V.3.7).

Wenn in einer solchen Art und Weise Kompetenzen der Rechtsdurchsetzung auf die Internetintermediäre verlagert werden – was »zur Norm in der staatlichen Internetregulierung« zu werden scheint – schafft dies zugleich »neue Herausforderungen hinsichtlich Effektivität, Transparenz und Verantwortlichkeit« (Küllmer/Breindl 2019: 338), denn letztlich werden sie damit »zu Kontrollinstanzen mit quasi-staatlichen Aufgaben« (ebd.: 349). Für den SRIW (2017: 5) »verpasst der Entwurf die Gelegenheit, ein System der Ko-Regulierung zu schaffen, das eine der Materie angemessene Aufteilung der Verantwortung zwischen Staat und Anbietern vornehmen würde.« Dagegen konstatierte Eifert (2018: 9f.), dass »die Ansätze des NetzDG mit den Vorgaben für eine strukturierte Verantwortungswahrnehmung von Plattform-Intermediären grundsätzlich den richtigen Weg« einschlagen und »paradigmatisch für die zukünftige Regulierung der Sozialen Netzwerke sein sollten.« Diese disparate Einschätzung findet sich auch jenseits des

NetzDG-Bezugs. Während Schulz und Held (2002: 1) zu Beginn der 2000er-Jahre am Untersuchungsbeispiel von Fällen aus dem Telekommunikations-, Medien- und Datenschutzrecht noch danach fragten, ob das »Konzept Regulierter Selbstregulierung den ›Dritten Weg‹ für die Steuerung in der Informationsgesellschaft bilden« könnte, wiesen Puppis et al. (2004: 10) bereits auf den auch in der Medienpolitik vollzogenen Wandel in der Steuerungsdimension hin: Staatlichkeit transformierte sich dahin gehend, dass »ein Vordringen des Selbstregulierungsprinzips als Steuerungsinstrument« feststellbar war. Und auch Küllmer und Breindl (2019: 348) konstatieren:

> »Die aktuelle Praxis in Deutschland zur Durchsetzung von Regulierung von Internetinhalten stützt sich vor allem auf die Regulierte Selbstregulierung der Internetindustrie in Kooperation mit den staatlichen Behörden.«

Mit Blick auf das NetzDG und den DSA scheinen gleichwohl beide Einschätzungen graduell miteinander vereinbar: Auf der einen Seite kann die Gesetzgebung als Übergang von der Selbstregulierung zur regulierten Selbstregulierung charakterisiert werden. Auf der anderen Seite sprechen die Diskussionen um die Privatisierung der Rechtsdurchsetzung und Rechtsetzung (siehe Kapitel V.3.5) für eine gleichzeitig stattfindende Stärkung der Selbstregulierungskapazität.

Zum Schluss dieses Kapitels soll noch kurz auf eine besondere Form der »Kooptation« von Unternehmen in der Rechtsdurchsetzung aufmerksam gemacht werden. Diese zeigt sich am Beispiel des Umgangs mit dem Messengerdienst Telegram im Rahmen des NetzDG. In diesem Fall nutzte der Staat quasi das Monopol der Anbieter:innen von Mobiltelefonbetriebssystemen und deren Souveränität über ihre Plattform beziehungsweise den App-Marktplatz aus. Zuvor war es dem Bundesamt für Justiz (BfJ) aufgrund fehlender Kontaktdaten des in Dubai ansässigen Telegram-Betreibers nicht möglich gewesen, die offiziellen Anhörungsschreiben bezüglich Verstöße (weder wurde eine behördliche Ansprechperson genannt noch ein Beschwerdeverfahren für strafbare Inhalte implementiert) gegen das NetzDG zuzustellen. Erst über Google und Apple kam die Behörde an eine ladungsfähige Anschrift des Unternehmens (vgl. Bewarder/Naber 2022). Zwar kam es im Anschluss zu Gesprächen zwischen Innen- und Justizministerium sowie Telegram, in denen das Unternehmen eine Kooperation und die Benennung eines direkten Ansprechpartners ankündigte (vgl. Neuerer 2022). Jedoch gab es im Anschluss keine Rückmeldung des Unternehmens, sodass sich das BfJ letztlich durch eine Veröffentlichung der Schreiben im Bundesanzeiger im März 2022 behalf. Damit galt dieses zwar als zugestellt, sodass Anhörung und Bußgeldverfahren starten konnten (vgl. Krempl 2022a). Der weitere Gang des Verfahrens und sein Ausgang bleiben zurzeit offen.

Jenseits dieses Sonderfalls hing die Kritik an der Privatisierung der Rechtsdurchsetzung im Rahmen des NetzDG aber auch mit den dort gesetzten Anreizen zusammen, die in Kombination mit plattformseitig eingesetzten (algorithmischen) Instrumenten als Gefahr für die Meinungsfreiheit gesehen wurden.

V.3.3.2 Overblocking und Zensur statt Meinungsfreiheit?

Der Umgang mit über internetbasierten Plattformen vermittelten Inhalten gestaltet sich generell auf drei Ebenen differenziert aus:

1. Art des Eingriffs: Inhalte können *gesperrt*, *entfernt* (gelöscht) oder verändert werden. Im Kontext von NetzDG und DSA spielen nur die ersten beiden Arten eine Rolle. Darüber hinaus kommt mit der Novellierung des NetzDG (siehe Kapitel V.3.4) die Frage der Weiterleitung rechtswidriger Inhalte und ihrer Verfasser:innen an Strafverfolgungsbehörden hinzu.[28]
2. Entscheidungsfindung: Die Entscheidung über die (Nicht-)Durchführung des Eingriffs (1.) kann *durch Menschen* oder automatisiert *durch Algorithmen* erfolgen.
3. Zeitpunkt des Eingriffs: Die Durchführung des Eingriffs (1.) kann manuell oder automatisch (2.) *vor* der Veröffentlichung (beim Upload) oder *nach* der Veröffentlichung (und Meldung beziehungsweise Beanstandung) erfolgen.

Die Kombination dieser Elemente mit anderen Vorgaben im NetzDG wurde frühzeitig, insbesondere von Bürger:innenrechtsorganisationen, als eine Gefährdung der Meinungsfreiheit aufgefasst. Die formulierte Kritik zog zwei Argumente heran: die gesetzten Anreize zum *overblocking* sowie die Installation einer *Zensurinfrastruktur* durch Algorithmen und Uploadfilter.

Zum overblocking – das auf der zweiten Ebene, der Entscheidungsfindung, angesiedelt ist – würde es dabei kommen, weil Plattformen mit erheblichen Bußgeldern von bis zu fünf Millionen Euro rechnen müssten (§ 4 Abs. 2), was zu sogenannten *chilling effects*[29] führt: Betreiber:innen würden im Zweifelsfall eher zu viele als zu wenige Beiträge sperren oder löschen.[30] Dies sei insbesondere deswegen der Fall, weil im NetzDG zwar von »offensichtlich rechtswidrigen Inhalt[en]« (§ 3 Abs. 2 Satz 2) gesprochen wird, dies gleichwohl aber eine entsprechende Bewertung und Einordnung durch die Plattform voraussetzt (die eigentlich durch Gerichte erfolgen müsste). Diese Unsicherheit kombiniert das NetzDG mit hohen Bußgeldern und einer kurzen Frist von 24 Stunden, um beanstandete Inhalte zu entfernen oder zu sperren. Erwartbar wäre daher ein über das

28 Dass die möglichen Eingriffe über ein Entfernen oder Sperren hinausgehen können, wird im DSA auch daran deutlich, dass nicht mehr wie zuvor im Rahmen von Inhaltsregulierungen von »notice and take down« (oder »notice and take down and stay down«) gesprochen wird, sondern allgemeiner von »notice and action« (Art. 14).

29 Nach Penney (2022: 1455, 1530) entstehen chilling effects im Kontext von Ambiguität und Ungewissheit und führen zu einem an (vermeintliche) soziale Normen *über*angepassten Verhalten, um rechtliche Konsequenzen zu vermeiden. Die Effekte umfassen sowohl Selbstzensur, wenn bestimmter Verhaltensweisen vermieden werden, als auch Selbstanpassung, im Sinne eines sozial angepassten Verhaltens, über das rechtlich notwendige Maß hinaus.

30 Die Bußgeldleitlinie des BMJ (2018: 8) legte explizit fest, dass »sich aus einer Häufung von Fehlentscheidungen innerhalb eines überschaubaren Zeitraums eine Indizwirkung dahin ergeben [könnte], dass die Vorgaben« für ein wirksames Verfahren nicht eingehalten werden und daher ein bußgeldbewehrter Tatbestand vorliegen könnte.

notwendige Maß hinausgehendes Blockieren *[overblocking]* eigentlich rechtskonformer Inhalte.

> »Der Dammbruch durch Meldungen von vermeintlich Betroffenen, die sich die kurzen Fristen und erheblichen finanziellen Risiken der Betreiber sozialer Netzwerke zu Nutze machen wollen, ist vorprogrammiert« (DGRI 2017: 10).

Zwar reichen die Daten (auf Grundlage der Berichtspflichten) beziehungsweise der Datenzugang bei den Plattformen nicht aus, um die tatsächliche Bedeutung von overblocking statistisch evaluieren zu können. Jedoch führte die Analyse der Anhaltspunkte für overblocking sowie vorhandener Studie bei Liesching et al. (2021: 143f.) insgesamt zu einer Bewertung, die eine reale Gefahr bestätigt:

> »Die Subsumtion der als Anhaltspunkte für Overblocking eruierten Kriterien deutet insgesamt eher darauf hin, dass das Netzwerkdurchsetzungsgesetz in dem […] befürchteten Sinne Anreize für eine schnelle Löschung von beschwerdegegenständlichen Inhalten auch in Zweifelsfällen setzt, die sich in der Anwendungspraxis realisiert haben könnten. Insgesamt sind für ein Overblocking im geschilderten Sinne mehr Anhaltspunkte ersichtlich als dafür, dass sich kein Overblocking im geschilderten Sinne zumindest teilweise etabliert hat.«

Die Gefahr einer Zensur(infrastruktur) kann auf den Ebenen 2 und 3 verortet werden. Auf Ebene 2 geht es um die Art der Entscheidungsfindung. Diese kann zum einen vollautomatisch erfolgen, etwa wenn bei audio-visuellen Medien mittels *fingerprinting*[31] ein erneuter Upload oder die Veröffentlichung bereits bekannten Materials verhindert wird. Über Machine-Learning-Algorithmen wird darüber hinaus versucht, unbekanntes Material zu klassifizieren.[32] Die Frage ist dann, ob dieses im Zweifelsfall gesperrt oder für eine manuelle Einordnung zurückgehalten wird. Insbesondere hier wird die Gefahr von overblocking und Zensur gesehen. Wenn keine algorithmenbasierte Erkennung erfolgt, kommen die sogenannten Content-Moderator:innen ins Spiel, die Inhalte nach vorgegebenen Regeln (beispielsweise anhand von Beispielleitfäden) bewerten und gegebenenfalls entfernen oder sperren.[33] Bei beiden Verfahren entscheiden private Akteure anstel-

31 Beim fingerprinting wird durch einen Algorithmus (ähnlich einer Hash-Funktion) ein eindeutiger Identifier für einen digitalen Inhalt (beispielsweise für ein Video) erstellt. Der Fingerabdruck (eine Folge alphanumerischer Zeichen) verbraucht (im Gegensatz etwa zu der Videodatei, die er repräsentiert) kaum Speicherplatz und ermöglicht es daher sehr effizient, einen Inhalt gegen eine Liste bekannter Inhalte auf Übereinstimmung abzugleichen.

32 Diese werden aber nicht nur genutzt, um unbekanntes Material zu klassifizieren. Sie sollen auch helfen, bekanntes Material in veränderten Kontexten zu erkennen. So wird etwa versucht, Fingerprinting-Algorithmen so zu gestalten, dass der Fingerabdruck sich auch bei leichten Abänderungen des Inhalts (etwa ein gekürztes, mit einem Rahmen versehenes oder im Bildausschnitt verschobenes Video) nicht verändert (zum technischen Hintergrund und zur Einschätzung siehe etwa Struppek et al. 2022).

33 Auf die dabei ebenfalls anzutreffende Problematik der teilweise prekären Arbeitsbedingungen und angesichts des mitunter schwer erträglichen und traumatischen Materials ungenügenden

le von Gerichten über die Rechtswidrigkeit von Inhalten. Reporter ohne Grenzen (2018) kritisierte daher das NetzDG scharf:

> »Die Bundesregierung hat mit dem NetzDG private Unternehmen zu Richtern über die Presse- und Informationsfreiheit im Netz gemacht, ohne eine öffentliche Kontrolle des Löschverfahrens sicherzustellen.«

Eng mit beiden Umsetzungsmöglichkeiten verbunden ist die Debatte um den Einsatz sogenannter Uploadfilter. Diese bezog sich nicht nur auf das NetzDG, sondern wurden besonders intensiv um Artikel 13 (später Artikel 17) der EU-Urheberrechtsreform 2019 geführt. Denn der Unterschied zwischen maschineller und manueller Content-Moderation liegt nicht nur im Einsatz von Algorithmen oder Menschen, sondern auch im Zeitpunkt ihres Einsatzes, womit wir uns auf der dritten Ebene befinden. Menschliche Moderation findet in der Regel ex post statt. Ein *bereits veröffentlichter* Inhalt wird nach dessen Meldung auf einen Verstoß gegen Community-Richtlinien oder strafrechtliche Tatbestände hin untersucht. Uploadfilter analysieren den Inhalt dagegen bereits während des »Uploads«, also *vor der Veröffentlichung*. Damit erfolgt eine Ex-ante-Prüfung, aus der sich auch die Verwendung des Zensurbegriffs[34] erklärte. Die Verbindung von Filterung und Zensurvorwürfen ist keine neue Entwicklung.[35]

Von Bürger:innenrechtsorganisationen wird in diesem Kontext darüber hinaus immer wieder vor dem Aufbau einer Zensur*infrastruktur* gewarnt.[36] Ein einmal für ein klar bestimmtes und eingegrenztes Ziel eingeführtes System (etwa gegen den Upload dokumentierten Kindesmissbrauchs) lässt sich, wenn es einmal implementiert wurde, einfach zu einem späteren Zeitpunkt durch Gesetzesänderungen auf andere Inhalte ausweiten.[37] Wenn die Erstellung der Filter und ihre Anwendung auf privatwirtschaftliche

---

psychologischen Betreuung wird an dieser Stelle nicht weiter eingegangen. Zur medialen Berichterstattung siehe beispielsweise Meineck (2021) und Peteranderl (2019).

34 Auch wenn das Grundgesetz (Art. 5 GG) »eine Zensur findet nicht statt« festschreibt, spricht dies nicht gegen eine staatliche Kontrolle *nach* der Veröffentlichung (wie sie bezogen auf Print- und Medienbereich etabliert ist). Den Kritiker:innen geht es daher bei der Zensurgefahr vor allem um die automatische Blockierung *vor* Veröffentlichung.

35 Bereits im 1989 als digitales Textdokument veröffentlichten »The Modem Dictionary« von R. Scott Perry (1993) findet sich unter dem Begriff »Filter« der Hinweis auf die Möglichkeit damaliger Mailbox-Systeme *[Bulletin Board System; BBS]*, unerwünschte Begriffe (insbesondere Schimpfwörter) automatisch zu löschen oder zu maskieren.

36 Aktuell findet diese Diskussion für das Client-Side-Scanning (CSS) im Zuge der sogenannte Chatkontrolle statt, die von der EU-Kommission (COM/2022/209 final) im Entwurf der Verordnung zum Kampf gegen Kindesmissbrauch vorgesehen ist (vgl. Europäische Kommission 2022c). Hierbei soll automatisiert auf den Endgeräten der Nutzer:innen jede Kommunikation (Text, Bild, Video) auf dokumentierten Kindesmissbrauch hin untersucht und bekanntes sowie verdächtiges Material an die Strafverfolgungsbehörden gemeldet werden (für die dagegen vorgebrauchte Kritik siehe beispielsweise Breyer 2022).

37 Bürger:innenrechtsorganisationen argumentieren darüber hinaus, dass gerade gesellschaftlich eindeutig geächtete Straftatbestände wie dokumentierter Kindesmissbrauch oder Terrorismus zur Einführung neuer Instrumente oder zur Umsetzung von Maßnahmen genutzt werden, weil so ein kritischer Diskurs erschwert wird (Küllmer/Breindl 2019: 348). Verunmöglicht wird er jedoch nicht, wie das Beispiel des »Gesetzes zur Bekämpfung von Kinderpornografie in Kommunikati-

Unternehmen übertragen wird, besteht des Weiteren keine (öffentliche) Transparenz darüber, wie diese stattfindet und damit darüber, was gefiltert wird – sofern hier keine entsprechende Regulierung erfolgt (siehe Kapitel V.3.7) (vgl. Küllmer/Breindl 2019: 348).

Im Entwurf des NetzDG war explizit verpflichtend vorgesehen, dass »sämtliche auf den Plattformen befindlichen Kopien des rechtswidrigen Inhalts ebenfalls unverzüglich« entfernt oder gesperrt (§ 3 Abs. 6) und »wirksame Maßnahmen gegen die erneute Speicherung des rechtswidrigen Inhalts« getroffen werden müssen (§ 3 Abs. 7). Zwar sind beide Vorgaben im verabschiedeten Gesetzestext nicht mehr enthalten, gleichwohl ist damit der Einsatz von Algorithmen zur Vorabprüfung durch die Plattformen keinesfalls ausgeschlossen. Damit besteht auch hier weiterhin die oben beschrieben Gefahr von overblocking, die allerdings bei einem Ex-ante-Vorgehen nur schwerlich erkannt werden kann, weil die geblockten Inhalte (außer der uploadenden Person) nie jemand wahrnehmen konnte (sieh hierzu insbesondere Kapitel VI.1.1.2 zur Governance by Algorithms).

Aus Steuerungsperspektive besteht also weiterhin die Möglichkeit *nicht intendierter Nebenwirkungen* (einer Einschränkung der Meinungsfreiheit) aufgrund von Fehlsteuerung im Sinne einer von der *erwarteten Steuerungswirkung abweichenden Reaktion* der Steuerungsadressaten (in Form von overblocking). Mit Blick auf die gleichwohl sichtbar werdenden neue Steuerungsinstrumente und -notwendigkeiten im digitalen Zeitalter stellt sich mithin die zentrale Frage, wie sich diese Governance *by* Algorithms durch eine Governance *of* Algorithms regulieren lässt (siehe Kapitel V.3.7).

Jenseits dieser Frage spielten einige der bereits zum Gesetzesentwurf formulierten Kritikpunkte auch bei der Novellierung des NetzDG eine Rolle.

V.3.4 Policy II: Novellierung des NetzDG

Die mit dem NetzDG beabsichtigte Steuerungswirkung trat nicht im erwünschten Umfang ein. So wurde 2019 das erste Bußgeld in Höhe von zwei Millionen Euro gegen Facebook verhängt, weil der Konzern seiner Berichtspflicht nur unvollständig nachkam. Darüber hinaus wurde im NetzDG zwar klar spezifiziert, innerhalb welcher Zeiträume rechtswidrige Inhalte auf der Plattform entfernt oder gesperrt werden müssen, es ließ aber offen, wie die geforderte Funktionalität, mit der Nutzer:innen der Plattform Inhalte melden können, ausgestalteter werde. Rieger und Sinders (2020: 24) weisen in diesem Zusammenhang darauf hin, dass fehlenden Vorgaben oder Richtlinien durch den Gesetzgeber zu sehr unterschiedlichen Implementationen bei den Plattformen geführt haben – mit erheblichen Auswirkungen auf das Nutzer:innenverhalten. Die nutzerunfreundliche Gestaltung der Meldefunktion, im Sinne eines »Dark Pattern«

onsnetzwerken« (Zugangserschwerungsgesetz) gezeigt hat (die der damals zuständigen Familienministerin Ursula von der Leyen zugleich den Spitznamen »Zensursula« einbrachte). In diesem Fall konnte mit der Formel »Löschen statt sperren« in Verbindung mit den Argumenten, dass die geplante Sperrung einfach zu umgehen sei und in Bezug auf den Straftatbestand ohnehin keine Schutzlücke bestehe, sogar durchgesetzt werden, das beschlossene Gesetz wieder zurückzunehmen (vgl. Scheffel 2016: 135–174).