Digital Services Act (DSA)
Vermeintliche Sicherheit statt Meinungsfreiheit?

Rebecca Hümmer, Beisitzerin im Bayerischen Landesvorstand des BSW

DAS – was ist das?

Der Digital Services Act (DSA) ist eine EU-Verordnung (EU) 2022/2065, die seit dem 17. Februar 2024 vollständig gilt.

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

https://gesetz-digitale-dienste.de/dsa/

Er schafft einen einheitlichen Rechtsrahmen für Vermittlungsdienste* sowie VLOPs/VLOSEs* mit abgestuften Pflichten je nach Rolle und Größe. Ziel ist, illegale Inhalte schneller über wirksame Notice-and-Action-Verfahren zu adressieren, Transparenz (z. B. Begründungspflichten, Reports, SoR-Datenbank) zu erhöhen und systemische Risiken (u. a. Grundrechte, Wahlen, öffentliche Sicherheit, Minderjährige) zu analysieren und zu mindern. Das gilt nicht nur für Meta, Google & Co., sondern auch für kleine Anbieter. Aber: Je größer, desto strenger.

Transparenzberichte, Melde- und Abhilfe-Systeme, Risikobewertungen, Risikominderung, Audits, Datenzugang für Forschende u. a. sind Pflicht und werden mit Strafen von bis zu 6 % des weltweiten Jahresumsatzes bei Verstößen geahndet. Der DSA soll, im besten Sinne ausgelegt, keine generelle Vorzensur darstellen. Das klingt vernünftig, hat aber Nebenwirkungen, die gerade legale (politische) Rede und kleine Anbieter treffen können. Genau an diesen Stellschrauben entscheiden sich in der Praxis Eingriffe in die Meinungsfreiheit und Ungerechtigkeiten gegenüber kleineren Unternehmen.

* „Vermittlungsdienste“: grundlegende Kategorie von Internet-Diensten, die Informationen zwischen Nutzern übertragen oder speichern. Art. 3 DSA unterscheidet drei Basistypen:

- Mere conduit (reine Durchleitung): bloßes Übertragen/Zurverfügungstellen von Zugang zu Netzen (Internetzugangsanbieter, Mobilfunknetze, Backbone/Peering, DNS-Resolver)
- Caching: Zwischenspeichern, um Übertragung zu beschleunigen (CDN-Knoten (Content Delivery Networks), Proxy-Caches)
- Hosting: Speichern von User-Inhalten (Webhosting, Cloud-Storage, Foren, Videoplattformen, soziale Netzwerke, Marktplätze, App-Stores) – Untergruppe: Online-Plattformen (z. B. Facebook, YouTube, TikTok, Marktplätze wie eBay/Kleinanzeigen).

* VLOP: Very Large Online Platform; VLOSE: Very Large Search Engine – eigene Kategorien im DSA

Aktueller denn je

Im Juli hat die EU-Kommission einen „Delegated Act“ eingesetzt https://netzpolitik.org/2025/zugang-fuer-forschung-so-muessen-online-dienste-ihre-datensilos-oeffnen/ (mehr dazu s. u.), mit dem erstmals verpflichtend interne Daten der Konzerne für „autorisierte Forschende“ zugänglich gemacht werden. Was als Transparenzmaßnahme serviert wird, wirft aber datenschutzrechtliche und demokratische Fragen auf: Wer kontrolliert diesen Zugriff? Nach welchen Kriterien erfolgt die Auswahl? Und was passiert mit diesen Daten?

Der neue Delegated Act ist allerdings nur die Spitze des Eisbergs. Der DSA wirkt nicht im luftleeren Raum. Er entsteht, wird ausgelegt und durchgesetzt in einem Netz aus politischen Interessen, Behördenpraxen und zivilgesellschaftlichen Akteuren. Wer diese Verflechtungen ignoriert, versteht nicht, warum seine Umsetzung problematisch sein kann.

DSA in der Kritik

Unbestritten sinnvoll sind klare Meldewege gegen illegale Inhalte im Internet (z. B. Terrorpropaganda, Darstellungen sexualisierter Gewalt gegen Kinder).

Gleichzeitig belegen Studien eine Häufung an Löschungen legaler Inhalte (Overblocking): In Frankreich, Deutschland, Schweden waren 87,5 – 99,7 % der gelöschten Kommentare rechtlich zulässig (s. u.); „awful but lawful“ fasst es schön zusammen. Das verschiebt Diskurse im Netz leise, aber spürbar.

Hinzu kommen strukturelle Bedenken: vage Begriffe (z. B. „systemische Risiken“), nach denen gehandelt und geprüft werden soll, Delegierte Rechtsakte ohne volle Parlamentsdebatte, und eine Durchsetzungsarchitektur (DSCs, Trusted Flaggers), die politische Einflussnahme nicht ausschließt.

Pflichten großer und kleiner Anbieter

Plattformen müssen leicht nutzbare Meldesysteme, transparente Begründungen für Moderationsentscheidungen, Widerspruchsmöglichkeiten und regelmäßige Berichte anfertigen. Sehr große Online-Plattformen (VLOPs) und Suchmaschinen (VLSEs) (z. B. Meta-Dienste, sehr große Marktplätze oder Videoplattformen wie YouTube, TikTok, LinkedIn, Wikipedia; Marktplätze wie Amazon oder AliExpress; sowie Suchmaschinen wie Google oder Bing) tragen zusätzliche Pflichten wie eine jährliche Risikobewertung; außerdem müssen Meldungen sog. „Trusted-Flagger“ (Erklärung s. u.) priorisiert behandelt werden(Art. 22), bleiben formal aber keine staatlichen Löschanordnungen.

https://gesetz-digitale-dienste.de/dsa/ v. a. Abschnitt 5 Art. 33 - 43

Diese Pflichten binden personelle Ressourcen, Budgets, Prozesse, was für Konzerne machbar ist, für Nischenanbieter allerdings schwierig.

Für kleine Plattformen, Start-ups und Community-Dienste – etwa eine lokale Kleinanzeigen-Seite, ein Discourse-Forum oder eine Mastodon-Instanz – gelten im DSA zwar formal abgespeckte Pflichten, die Grundlogik bleibt aber gleich: Es braucht funktionierende Meldesysteme und „Notice-and-Action"-Prozesse, nachvollziehbare Begründungen bei Moderationsentscheidungen sowie Möglichkeiten zum Widerspruch (vgl. Art. 11–15, 16–18; für Online-Plattformen zusätzlich Art. 20–28). Gleichzeitig sieht der DSA Erleichterungen für Kleinst- und Kleinunternehmen vor (Art. 29): Wer weniger als 20 Beschäftigte hat und unter 2 Mio. € Jahresumsatz liegt (Kleinstunternehmen) bzw. weniger als 50 Beschäftigte und unter 10 Mio. € Umsatz (Kleinunternehmen), ist von einem ganzen Bündel an Plattformpflichten ausgenommen. Dazu zählen insbesondere das interne Beschwerdemanagement (Art. 20), die außergerichtliche Streitbeilegung (Art. 21), die Priorisierung von Trusted-Flagger-Meldungen (Art. 22), Missbrauchsmaßnahmen (Art. 23), Transparenzberichte (Art. 24), Interface-Vorgaben (Art. 25), Werbe-Transparenz (Art. 26), Recommender-Transparenz (Art. 27) und Jugendschutzpflichten (Art. 28). Für Online-Marktplätze entfallen in dieser Größenklasse zudem die Händler-Nachverfolgbarkeit/KYC (Art. 30), „Compliance by design" (Art. 31) sowie Informationspflichten gegenüber Käuferinnen und Käufer bei illegalen Produkten oder Diensten (Art. 32). Unterm Strich verlangt der DSA also auch von kleinen Anbietern rechtsstaatliche Mindestprozesse, verschont sie aber in der Aufbauphase vor den kostenintensivsten Compliance-Bausteinen großer Plattformen.

Folgen

Praktisch führen die anspruchsvollen Pflichten für Anbieter zu einer internen Risikovermeidung in Form einer restriktiveren Moderation, präventivem Löschen, Geo-Blocking, Verzicht auf kontroverse Diskursformate. Oft fehlen hierzu, gerade bei den „Kleinern", schlicht Personal, Juristen und Trust&Safety-Tools. Es entsteht somit entweder eine hohe Kostenlast oder Marktkonzentration zugunsten der Großen.
Ein wohl unerwünschter Nebeneffekt, forciert durch die Entbindung von Pflichten wie Beschwerdemanagement und Trusted Flagger-Nachverfolgung, ist sicher, dass diese kleinen Plattformen und Communities zunehmend Nutzer anziehen, die sich vom streng moderierten Mainstream sozialer Netzwerke abwenden. Diese digitale „Selbstverlagerung" führt dazu, dass sich Gruppierungen mit Rand- oder Extrempositionen in abgeschlossenen Räumen versammeln, wo kaum externe Kontrolle oder Gegenrede stattfindet. Ein Beispiel dafür ist die Plattform Gab, die ursprünglich als freie Alternative zu Twitter startete und sich zu einem Sammelbecken für rechtsextreme und verschwörungsideologische Inhalte

entwickelte. https://en.wikipedia.org/wiki/Gab_(social_network)
Diese Isolation verstärkt natürlich Radikalisierungstendenzen: Fehlende Widersprüche normalisieren extreme Ansichten, während sich innerhalb der Gruppen ein geschlossenes Weltbild bildet. Der DSA adressiert solche Effekte bislang kaum, weil er kleine Anbieter zwar regulatorisch entlastet, aber keine Strategie vorsieht, um den gesellschaftlichen Folgen einer Fragmentierung des öffentlichen Diskurses entgegenzuwirken.

Digital Service Coordinator zur Durchsetzung des DSA

Der Digital Services Coordinator (DSC) ist die zentrale nationale Behörde zur Umsetzung des Digital Services Act in jedem EU-Mitgliedstaat. In Deutschland übernimmt diese Rolle seit Mai 2024 die Bundesnetzagentur.
https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs
https://www.dsc.bund.de/DSC/DE/_Home/start.html?r=1

Zum 1. Juli 2025 übernahm Johannes Heidelberger die Leitung des DSC. Er wurde auf Vorschlag des Präsidenten der Bundesnetzagentur Klaus Müller (B. 90/Grüne) vom Bundeskabinett bestätigt und durch den Bundespräsidenten berufen. Heidelberger ist seit 2012 unter anderem als Referatsleiter für Digitalisierung, Vernetzung und Internetplattformen bei den Bundesnetzagentur tätig. Er folgt auf Klaus Müller, der den DSC seit Mai 2024 kommissarisch leitete.

https://de.wikipedia.org/wiki/Klaus_M%C3%BCller_%28Politiker%2C_1971%29

Die Bundesnetzagentur ist eine selbstständige Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Wirtschaft und Energie (teilweise auch unter Fachaufsicht des Bundesministeriums für Digitales und Verkehr). Sie unterliegt der ministeriellen Rechts- und Fachaufsicht, ist aber in vielen sektorspezifischen Regulierungsentscheidungen gesetzlich zur Unabhängigkeit verpflichtet. Die BNetzA ist also aufsichts- und teilweise weisungsgebunden, aber es bestehen gesetzliche Schranken der politischen Einflussnahme bei fachlich-regulatorischen Entscheidungen.

https://www.bundestag.de/resource/blob/529464/17d91d69577a4b1697c7c012218ed18b/wd-3%E2%80%93158%E2%80%9317-pdf-data.pdf

Trotzdem: Entscheidungen darüber, wie der DSA umgesetzt wird und welche Organisationen als Trusted Flagger anerkannt werden und damit bevorzugt Löschmeldungen an Plattformen übermitteln dürfen, wer Forschungszugänge erhält, wie mit Beschwerden verfahren wird usw. obliegen allein dieser einen Instanz. Kritiker wie Wolfgang Kubicki (FDP) warnten daher in der letzten Legislaturperiode vor einer „Zensurbehörde der Grünen“ unter Wirtschaftsminister a. D. Robert

Habeck und dem o. g. ehem. Leiter des DSC Klaus Müller (ebenfalls B90/Grüne). Auch wenn diese Formulierung polemisch ist, bleibt die strukturelle Schwäche bestehen: Eine inhaltlich hochbrisante und auch politische Aufgabe liegt bei einer Behörde, die vermeintlich nicht komplett unabhängig arbeitet.

Bei der Umsetzung des DSA arbeitet der deutsche Digital Services Coordinator, alias Bundesnetzagentur eng mit der Bundeszentrale für Kinder- und Jugendmedienschutz, der Landesanstalt für Medien NRW (als gemeinsame Beauftragte der Landesmedienanstalten), dem BfDI (unabhängige Aufsichtsbehörde des Bundes für Datenschutz), der EU-Kommission und den DSCs der anderen Mitgliedstaaten zusammen. Das ist sinnvoll, birgt aber wiederum Risiken. Viele Schnittstellen nämlich bedeuten potenzielle Reibungsverluste, so uneinheitliche Maßstäbe für Jugendschutz, Datenschutz und Plattformaufsicht. Dies wiederum erfordert erhöhte Anforderungen an die transparente Handhabung.

Die europäische Zuständigkeitsverteilung schafft zusätzliche Brisanz. Setzt die Idee des DSA auf einen EU-weiten Kooperationsmechanismus unter Leitung des European Board for Digital Services, steht dem entgegen, dass zum jetzigen Zeitpunkt mehrere Mitgliedstaaten noch keine voll handlungsfähigen DSCs aufweisen können, was die einheitliche und schnelle Durchsetzung des DSA freilich erschwert. Besonders bei grenzüberschreitender Desinformation kollidieren die Verfahren (Prüfung, Anhörung, Einspruch) mit der hohen Verbreitungsgeschwindigkeit in sozialen Medien.

Weil Meta, Google, TikTok u. a. ihren EU-Sitz in Irland haben, liegt die praktische Aufsicht für diese Plattformen häufig beim irischen DSC (Coimisiún na Meán), einer Behörde, die bereits in der DSGVO-Praxis für zögerliche Verfahren gegenüber Großunternehmen kritisiert wurde. Grenzüberschreitende Fälle laufen damit oft über Dublin; Kontrolle und Aktionen in kritischen Momenten können ergo leicht zu spät zu kommen und ins Leere laufen.

Am 12. August hat der DSC seinen ersten Tätigkeitsbericht für das Berichtsjahr 2024 vorgelegt.

https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2025/20250812_DSC_Taetigkeitsbericht.html

Seit der Einrichtung im Mai 2024 verzeichnete der DSC 824 Beschwerden zu möglichen DSA-Verstößen; 87 Fälle wurden nach dem Sitzlandprinzip an andere EU-Koordinatoren weitergegeben. Im nationalen Zuständigkeitsbereich leitete die Behörde bis Jahresende vier Verwaltungsverfahren gegen Vermittlungsdienste* ein und wirkte zudem in Verfahren der EU-Kommission u. a. gegen AliExpress, Temu,

TikTok und X mit. Bußgelder und Sanktionen wurden allerdings keine verhängt. Neben der Beschwerdebearbeitung baute der DSC zentrale Strukturen für die deutsche DSA-Durchsetzung auf. 2024 wurde die User Rights GmbH als erste außergerichtliche Streitbeilegungsstelle anerkannt und REspect! als Trusted Flagger zertifiziert. Insgesamt zeigt der Bericht ein Anlaufjahr mit bereits hohem Beschwerdevolumen und einigen Zertifizierungsprozessen.

Trusted Flagger

Der Digital Services Act sieht vor, dass jeder EU-Mitgliedstaat-DSC ausgewählte Organisationen oder Stellen als Trusted Flagger („vertrauenswürdige Hinweisgeber“) zertifiziert. Diese Trusted Flagger sind NGOs und Verbände, die durch ihren Status einen priorisierten Kanal zu Plattformen erhalten, um Auffälligkeiten zu melden. Sie genießen also besondere Privilegien, da Plattformen ihre Meldungen vorrangig bearbeiten müssen. In Deutschland hat der DSC bisher REspect! (Meldestelle gegen Hetze im Internet), HateAid GmbH (Unterstützung für Betroffene digitaler Gewalt), vzbv (Verbraucherzentrale Bundesverband e.V.), BVOH (Bundesverband Onlinehandel e.V., Interessenvertretung des E-Commerce-Sektors) zertifiziert. https://www.dsc.bund.de/DE/TrustedFlagger/trusted_flagger_node.html

Die Idee dahinter ist nicht schlecht: Trusted Flagger sollen über besondere Expertise verfügen – zum Beispiel im Bereich Jugendschutz, Terrorismusbekämpfung oder Hassrede – und daher qualitativ hochwertige Hinweise geben, die die Plattformen entlasten; Expertise und Qualität statt Massenmeldungen also.

In der Realität aber besitzen diese Meldestellen keine demokratische Legitimation, ihre Auswahlkriterien sind nur begrenzt transparent, so auch die Finanzierungsunabhängigkeit – das alte NGO-Debakel. Dennoch tragen sie faktisch zur Kontrolle öffentlicher Inhalte, konkret bzgl. Äußerungen und Inhalten in sozialen Medien, bei und nehmen somit Einfluss auf deren Sichtbarkeit. Studien und Analysen (s. u.) sehen hier einen Treiber für Over-Removal (übertriebene Löschung), denn die Plattformen folgen oft schnell und ohne zusätzliche Prüfung diesen priorisierten Meldungen; aus Compliance-Furcht ab. Zudem zeigt der Fall der NGO REspect!, wie schnell die Unabhängigkeit der Trusted Flagger infrage gestellt werden kann und wie dünn der öffentliche Kontrollrahmen ist (mehr dazu s. u.)

Kontrolle und Ernennung von Trusted Flaggern

Trusted Flagger sind verpflichtet, jährlich Bericht zu erstatten. Die Bundesnetzagentur soll überwachen, ob ihre Arbeit sorgfältig und korrekt erfolgt. Werden Missbrauch, fehlerhafte Benachrichtigungen oder mangelnde Präzision festgestellt, kann der Status ausgesetzt oder entzogen werden.
In Deutschland liegt die Zuständigkeit für die Zertifizierung der „vertrauensvollen

Hinweisgeber“ wie erwähnt allein bei der Bundesnetzagentur als DSC. Sie entscheidet, wer diesen privilegierten Status erhält und kann die Zertifizierung auch wieder entziehen.

Was müssen Trusted Flagger vor ihrer Zertifizierung vorweisen? Das ist zum einen der Nachweis besonderer Fachkenntnisse in der Erkennung illegaler Inhalte. Zum anderen ihre Unabhängigkeit; es darf kein organisatorisches oder wirtschaftliches Abhängigkeitsverhältnis zu Plattformen geben. Und schließlich müssen sie nach etablierten Standards arbeiten und ihre Meldungen sorgfältig und faktenbasiert prüfen.

EU Digital Strategy – Trusted Flaggers

https://www.dsc.bund.de/DSC/DE/4TrustedF/start.html

Da die Trusted Flaggers wie erwähnt nicht demokratisch legitimiert sind, sondern allein von der Bundesnetzagentur zertifiziert werden, ist es umso bedenklicher, dass ihre Meldungen unmittelbare Folgen für die Sichtbarkeit oder Löschung von Inhalten im Netz haben.

Sogar die CDU-Abgeordnete Saskia Ludwig warnte gegenüber Euronews, halbstaatliche Melde-Organisationen als Rede-Schiedsrichter zu betrauen, berge ernste Risiken. So auch der Jurist Ralf Höcker: „Trusted Flagger sind umstritten, weil es halbstaatliche Organisationen sind, die mit staatlichen Mitteln zumindest zum großen Teil finanziert werden Staat finanziert werden und die de facto darüber entscheiden, welche Äußerungen im Internet legal sind und welche nicht legal sind. Das ist eine Form von staatlicher Zensur; man kann es Wahrheitsministerium nennen“. https://www.euronews.com/my-europe/2025/08/05/german-politicians-and-lawyers-worry-trusted-flaggers-of-online-hate-may-curb-freedom-of-s

Der genannte Euronews-Beitrag beschreibt die wachsende Sorge von Juristen und Politikerinnen, dass staatlich (mit-)finanzierte Meldestellen – inzwischen teils als Trusted Flagger zertifiziert – Meinungen fälschlich als Hass einstufen und damit DSA-Meldeketten auslösen. Geht eine Meldung eines Trusted Flaggers ein, müssen Plattformen zügig prüfen, entscheiden und einen Statement-of-Reasons-Eintrag hinterlassen. In der Praxis kann das – zumal unter Bußgelddruck – zu übervorsichtiger Moderation führen, was auch regierungskritische Memes trifft. Explizit soll hier auch auf die Fälle in Deutschland mit Polizeimaßnahmen nach Anzeigen im Sinne von §188 StGB hingewiesen werden. Ganz deutlich wird also, dass Meldungen aus dem DSA-Ökosystem in Strafverfahren für Bürgerinnen und Bürger münden können, obwohl der DSA das nicht fordert. Genau hier entsteht die politisch brisante Verbindung: Trusted-Flagger-Priorisierung zusammen mit nationalen Strafnormen (z. B. § 185/§ 188 StGB) und schnellen Plattformentscheidungen bergen das Risiko einer faktisch politisierten

Inhaltsdurchsetzung – besonders, wenn Auswahl, Finanzierung und Fehlerraten der Meldestellen nicht transparent sind.

Ein 2024 veröffentlichter Bericht des Think Tanks *Future of Free Speech* (s. u.) zeigt, dass in Frankreich, Deutschland und Schweden 87,5 bis 99,7 % der im Rahmen des DSA gelöschten Inhalte rechtlich zulässig gewesen wären.

Das Phänomen nennt sich Overblocking. Es entsteht, wenn Plattformen aus Angst vor Sanktionen zu viele Inhalte entfernen. Zwar haben Trusted Flagger keine Anordnungsbefugnis gegenüber Plattformen. Sie können lediglich auf mutmaßlich illegale Inhalte hinweisen; die Entscheidung über Löschung oder Sperrung trifft die Plattform selbst. Der privilegierte Meldeweg und die Möglichkeit von Sanktionen führt in der Praxis aber dazu, dass diese Meldungen oft sehr schnell und ohne eingehende Prüfung seitens der Plattformen umgesetzt werden.

Das REspect!-Problem

Die Vergabe des Trusted-Flagger-Status ist neben den teilweise „halbstaatlich“ finanzierten NGOs auch von weiterer politischer Brisanz. In Deutschland wurde 2024 als erster Trusted Flagger die Meldestelle REspect! zertifiziert – eine Organisation, die sich gegen Hassrede engagiert, aber wegen politischer Nähe zu einzelnen Regierungsakteuren in der Kritik steht.
Besonders umstritten war ein Foto des ehem. Leiters Ahmed Gaafar mit dem Großimam Ahmed al-Tayyib, der international für homophobe und antisemitische Äußerungen und seine Hamas-Nähe in der Kritik steht. Forderungen hinsichtlich einer **Überprüfung** durch die BNetzA wurden laut; eine konkrete Sanktion gegen REspect! oder eine Aberkennung des Staus sind nicht dokumentiert.

https://www.faz.net/pro/digitalwirtschaft/plattformen/die-trusted-flagger-und-die-meinungsfreiheit-in-der-eu-110049097.html

Dennoch steht im offiziellen „Leitfaden zur Zertifizierung als Trusted Flagger“ der Bundesnetzagentur ausdrücklich, dass der DSC die vorgelegten Informationen fortlaufend bewertet und „in Fällen, in denen nach einer Untersuchung festgestellt wird, dass ein Trusted Flagger die Zertifizierungsbedingungen nicht mehr erfüllt, die Zertifizierung widerrufen“ wird.
https://www.dsc.bund.de/DSC/DE/4TrustedF/leitfaden.pdf?__blob=publicationFile&v=3 Ob dem hinreichend nachgekommen wurde, ist fraglich.

Nutzerrechte & Schlichtung

Die User Rights GmbH ist bislang einzige anerkannte außergerichtliche Schlichtungsstelle, an die sich Nutzer wenden können – allerdings nur für Instagram, TikTok, LinkedIn; Beschwerden über andere Plattformen wie X oder Facebook sind momentan noch nicht möglich.

https://www.rnd.de/digital/beschwerdestelle-fuer-soziale-medien-nette-idee-aber-YW6BFAQMGBERVBWWTHGPYC6Z3E.html
Jugend- und Datenschutz, Urheberrecht oder Pornografie sind als große und wichtige Themen explizit von der Schlichtung durch User Rights ausgenommen. Es lässt sich festhalten: Der Wirkungsbereich dieser Schlichtungsstelle ist begrenzt.

Beschwerden von Usern werden zudem durch umfangreiche Formulare erschwert und es kommt noch dazu, dass die Entscheidungen der Schlichtungsstelle rechtlich nicht bindend sein. Für die Plattformen heißt das, dass sie den Beschlüssen gar nicht Folge leisten müssen; dies beruht auf Freiwilligkeit.

Wolfgang Kubicki (FDP) hat sich recht treffend dazu geäußert. Er hält „die Beauftragung eines privaten Dritten, der über ein zentrales Element unserer freiheitlichen Demokratie richten soll, für unerträglich“.
https://www.handelsblatt.com/politik/deutschland/kubicki-wirft-bundesnetzagentur-zensur-vor-spd-und-gruene-widersprechen/100077731.html

Delegated Acts

Über Delegierte Rechtsakte „kann der Kommission die Befugnis übertragen werden, Rechtsakte ohne Gesetzescharakter mit allgemeiner Geltung zur Ergänzung oder Änderung bestimmter nicht wesentlicher Vorschriften des betreffenden Gesetzgebungsaktes zu erlassen.“ (Art. 290 AEUV)

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A12008E290%3Aen%3AHTML&
Der EU-Kommission ist also erlaubt, Details einer bereits beschlossenen Verordnung (wie dem DSA nach Art. 87) später selbst festzulegen oder zu ändern – ohne ein neues, volles Gesetzgebungsverfahren; in unserem Falle z. B. Vorgaben zu Transparenzberichten, Audits oder – wie jüngst geschehen – zum Forschungszugang. Parlament und Rat können zwar widersprechen oder die Delegation widerrufen, sind aber nicht Mit-Gesetzgeber.

Der DSA ist als EU-Verordnung ausgestaltet und gilt damit in allen Mitgliedstaaten unmittelbar. Auch hierin können technische oder inhaltliche Details (z. B. Trusted Flagger Art. 22, Transparenzberichte Art. 24, Risikobewertung Art. 34) ohne einen neuen Parlamentsbeschluss mit delegierten Rechtsakten geltend gemacht werden (Art. 87 DAS); Parlament und Rat können allenfalls innerhalb einer gewissen Frist Einspruch erheben.

Zugang für Forschende

Am 1. Juli 2025 erließ die Kommission den Delegate Act C(2025)4340, der die Verfahren für den Datenzugang von Forschenden in sehr große Online-Plattformen (VLOPs) und Suchmaschinen (VLSEs) regelt (Art. 40 DSA) und Ende Oktober 2025 in Kraft treten soll. Das Ziel: Bewertung von systemischen Risiken. Dazu zählen unter anderem die Verbreitung illegaler Inhalte, Desinformation, Beeinträchtigung demokratischer Prozesse oder Gefahren für den Jugendschutz.

https://digital-strategy.ec.europa.eu/en/news/commission-adopts-delegated-act-data-access-under-digital-services-act

Zuständig für deutsche Anträge für Forschende ist die BNetzA/DSC. Begrüßenswert daran ist, dass mehr Forschung zu systemischen Risiken wie Wahlbeeinflussung und gezielten Hasskampagnen stattfinden kann. Unabhängige Datenanalysen helfen dabei, Missstände frühzeitig aufzudecken.

Kritisch jedoch sind die weiten Begriffe und Definitionen, nach denen die Forschung stattfinden soll: „systemische Risiken“ oder „öffentliche Sicherheit“ lassen großen Spielraum für Interpretation.

Durch komplexe Antragswege ergibt sich de facto eine Benachteiligung kleinerer Forschungseinrichtungen. Auch Universitäten mit begrenzten Ressourcen könnten z. B. Schwierigkeiten haben, die aufwendigen Antrags- und Datenschutzvorgaben zu erfüllen. Große, gut vernetzte Institutionen hätten damit einen Wettbewerbsvorteil.

https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/von-hoffnungen-und-hindernissen

Der Antragsprozess unterliegt – wenig überraschend – der Kontrolle des DSC bei der Bundesnetzagentur als Gatekeeper. Das wirft Fragen auf: Werden kritische Forschungsprojekte, die beispielsweise die Wirkung staatlicher Informationskampagnen oder die Arbeit der Trusted Flagger untersuchen, mit derselben Offenheit behandelt wie Projekte, die sich gegen „offensichtliche“ Desinformation richten?

Zu nennen sei noch das Risiko, dem sich Nutzer ausgesetzt sehen, da ihre Privatsphäre trotz der im Rechtsakt vorgeschriebenen Schutzmaßnahmen in Mitleidenschaft gezogen werden könnte, z. B. durch fehlerhafte Anonymisierung.

Unterm Strich ist der Forschungszugang im DSA grundsätzlich sinnvoll, doch der dazu erlassene Delegated Act gibt der EU-Kommission die Macht, über detaillierte Verwaltungsregeln den Rahmen wissenschaftlicher Arbeit festzulegen – ohne echte parlamentarische Mitbestimmung. „Stille Gesetzgeber“ wird das oft genannt: Die Kommission (und national die DSCs) entscheiden mit Antragsauflagen, Anerkennungskriterien und Sicherheitsvorgaben darüber, wer welche Plattformdaten wofür bekommt. Das kann Forschung indirekt steuern, kleinere Einrichtungen benachteiligen und sensible Themen ausbremsen.

Überblick: Relevante Studien zu Overblocking & Co.

Es lohnt sich der Blick in die Daten statt nur in die Gesetzestexte. Seit 2024 liegen mehrere empirische Analysen vor, die, aus unterschiedlichen Perspektiven, denselben Kern haben: Unter Druck werden viele Inhalte entfernt, obwohl sie rechtlich zulässig gewesen wären. Das deutet auf Overblocking hin, also eine vorsorgliche Übermoderation aus Risikoangst, die besonders kontroverse, aber erlaubte Meinungen trifft. Eng gesetzte Fristen und priorisierte Meldestrukturen legen den Grundstein für Fehler. Die folgenden Studien bilden den aktuellen Stand ab; weitere Arbeiten liefern Kontext zu Transparenzdefiziten, algorithmischer Willkür und den Präferenzen der Nutzerinnen und Nutzer.

Thema Overblocking

1. Think-Tank-Report (Vanderbilt University – The Future of Free Speech), *Preventing 'Torrents of Hate' or Stifling Free Expression Online?* (Mai 2024)
   Der Bericht analysiert gelöschte Kommentare auf Facebook und YouTube in **Frankreich, Deutschland, Schweden** (Datenerhebung Juni/Juli 2023; 60 große Pages/Channels; juristische Prüfung der Rechtmäßigkeit). Zentrales Ergebnis: **87,5 % bis 99,7 %** der gelöschten Kommentare waren **rechtlich zulässig**; in **Deutschland** lagen die Anteile am höchsten (**99,7 % Facebook**, **98,9 % YouTube**). Der Report interpretiert das als Hinweis auf **Overblocking** im Umfeld von NetzDG/DSA.
   https://futurefreespeech.org/wp-content/uploads/2024/05/Preventing-Torrents-of-Hate-or-Stifling-Free-Expression-Online-The-Future-of-Free-Speech.pdf

   „Tech Policy Press-Analyse (Mchangama, 24. Juni 2024): *Most Comments Deleted … Were Legal Speech — Why That Should Raise Concerns for Free Expression Online* – journalistischer Policy-Beitrag, der Ergebnisse des Future-of-Free-Speech-Reports zusammenfasst und deren Bedeutung für die Meinungsfreiheit diskutiert: Übervorsichtige Moderation kann **Chilling Effects** erzeugen und den **öffentlichen Diskurs** verengen. Der Artikel würdigt, dass der DSA **Transparenz- und Beschwerderechte** stärkt, warnt aber vor **Ausweitungen** (z. B. „European Democracy Shield") mit möglichen Eingriffen in freie Rede.
   https://www.techpolicy.press/most-comments-deleted-from-social-media-platforms-in-germany-france-and-sweden-were-legal-speech-why-that-should-raise-concerns-for-free-expression-online/

2. AlgoSoc-Policy-Report, Mai 2024
   Vergleich der Moderationspraxis und -geschwindigkeit im DSA-Kontext; ungleiche Reaktionsfristen drängen Plattformen in Richtung stärkerer

Automatisierung und erhöht damit das Risiko von Fehlentscheidungen/Overblocking.
https://algosoc.org/results/content-moderation-and-platform-observability-in-the-digital-services-act

Thema DSA-Transparenzdaten (Statement-of-Reasons/SoR) & Messprobleme

4. arXiv-Preprint: Shahi et al. (2025), „A Year of the DSA Transparency Database“
   Analyse von 1,58 Mrd. Moderationsakten aus der **DSA Transparency Database** rund um die Europawahl 2024: kaum Verhaltensänderungen der Plattformen sichtbar; erhebliche Transparenz-/Vergleichbarkeitsdefizite der SoR-Daten (erschwert belastbare Vergeliche); Moderationspraxis der Plattformen wurde rund um die Wahl kaum angepasst (positiv).
   https://arxiv.org/abs/2504.06976
5. Trujillo et al. (2025), „Auditing Self-reported Moderation Actions…“ ACM-Publikation, Mai 2025
   Prüft Konsistenz der Selbstberichte ider SoR-Daten gegenüber Plattform-Transparenzberichten: findet Lücken/Inkonistenzen zwischen SoR-Daten und Transparenzberichten – Overblocking-Studien, die sich nur auf Auswertung der SoR beziehen, können verzerrt sein.
   https://dl.acm.org/doi/10.1145/3711085
6. Internet Policy Review (2025, Special-Issue)
   Zeigt, dass Moderationsentscheidungen EU-weit weitgehend uniform ausgerollt werden (wenig Territorialisierung), was kulturelle/kontextuelle Nuancen unterbelichtet und Fehlentscheidungen wahrscheinlicher macht. Außerdem: SoR-Schema erschwert differenzierte Auswertungen (z. B. Unterscheidung zertifizierter Trusted Flagger)
   https://policyreview.info/articles/analysis/platform-observability-and-content-governance

DSA aus Sicht des BSW

Das BSW steht für ein digitales Gemeinwesen, das Sicherheit und Freiheit zugleich schützt: Illegale Inhalte sollen zügig entfernt und geahndet werden, legitime – auch scharfe – politische Rede muss sichtbar bleiben. Verfahren müssen neutral, transparent und überprüfbar sein; Pflichten verhältnismäßig, damit nicht nur Konzerne, sondern auch kleine und gemeinwohlorientierte Anbieter bestehen können. Staatliche Eingriffe sind klar zu begrenzen, Entscheidungen nachvollziehbar

zu begründen, Rechtsmittel schnell und wirksam zu gestalten – nur so entsteht Vertrauen statt schleichender Selbstzensur.

Vor diesem Maßstab ist der DSA kritisch zu prüfen. Die Meinungsfreiheit gerät unter Druck, wenn Vorsichtslöschungen und intransparente Eingriffe faktisch wie Zensur wirken. Die Vorrangspur für Trusted Flagger kann politisch oder persönlich motivierte Fehlmeldungen begünstigen. Diese und andere Kritikpunkte wurden in diesem Text ausführlich erläutert.

Warum es jetzt klare Korrekturen braucht

Ich halte den Digital Services Act für ein notwendiges, aber gefährlich unausgereiftes Regelwerk. Er zeigt, dass Europa seine digitale Souveränität ernst nehmen will, doch er droht, das zu verlieren, was ihn stark macht: das Vertrauen in demokratische Prozesse und den Schutz individueller Freiheit. Wer den digitalen Raum reguliert, ohne klare Begriffe und transparente Verfahren, öffnet politischen Deutungen Tür und Tor. Genau das geschieht derzeit.

Deshalb braucht es schnelle, gezielte Nachbesserungen. Begriffe wie „Desinformation“, „systemisches Risiko“ oder „öffentliche Sicherheit“ müssen enger definiert werden, damit sie nicht von Behörden oder NGOs nach eigenem Ermessen ausgelegt werden können. Ebenso dringend ist der Einbau ausdrücklicher Schutzklauseln für legale politische Rede. Sie dürfen nicht durch übervorsichtige Moderation oder algorithmische Vorfilterung unterdrückt werden.

Die Trusted Flagger sind ein weiteres Beispiel, wie gute Absichten in intransparente Macht umschlagen können. Wer privilegiert melden darf, muss sich öffentlicher Kontrolle stellen. Das heißt, ein Register zu Finanzierung, Governance und politischen Verbindungen, nachvollziehbare Fehlerquoten, unabhängige Audits und ein sofortiger Entzug des Status bei wiederholten Fehlmeldungen. Wir haben ein Recht zu wissen, welche Organisation welche Inhalte gemeldet hat und mit welchen Konsequenzen.

Auch Rechtsmittel müssen alltagstauglich werden: schnelle Fristen, klare Begründungen, leicht verständliche Verfahren und die Möglichkeit, gelöschte Beiträge vorläufig wiederherzustellen, wenn offensichtliche Fehler vorliegen. Das wäre kein Zugeständnis, sondern eine Rückbesinnung auf rechtsstaatliche Prinzipien.

Transparenzdaten wie die „Statement of Reasons“-Einträge gehören in die Öffentlichkeit. Sie müssen qualitätsgesichert, vergleichbar und über Dashboards für Interessierte, Forschende und Journalisten zugänglich sein. Nur so entsteht echte Plattformaufsicht.

Außerdem darf Forschung kein Privileg großer Institute werden. Auch unabhängige Teams und Universitäten brauchen realistische Chancen, Datenzugang zu erhalten und zwar ohne politisches Wohlwollen, aber unter Einhaltung hoher Datenschutzstandards.

Schließlich muss die Schnittstelle zum Strafrecht dringend überprüft werden. Wenn Hausdurchsuchungen wegen politischer Memes stattfinden, muss klar offengelegt werden, ob die zugrunde liegende Meldung von einem Trusted Flagger kam – und ob dieser möglicherweise einer politisch entgegengesetzten Richtung angehört.

Diese Reformen sind kein Angriff auf den DSA, sondern wären vielleicht seine Rettung. Nur wenn Transparenz, Verantwortung und Rechtsstaatlichkeit Vorrang haben, kann Europa glaubwürdig behaupten, im digitalen Raum Freiheit und Demokratie zu verteidigen.