Öffentlicher Appell gegen staatlich verknüpfte Identitätspflichten im digitalen Diskursraum

An Betreiber allgemeiner digitaler Diskursplattformen sowie an die European Board for Digital Services[1], die nationalen Digital Services Coordinators[2] und die zuständigen Datenschutzaufsichtsbehörden[3]

Digitale Diskursplattformen sind kein amtliches Verfahren, kein Bankzugang und kein Grenzübertritt. Sie sind Räume öffentlicher oder halböffentlicher Rede. Für die ordentliche Teilnahme an solchen Räumen, insbesondere für Posten, Antworten, Folgen, Auffindbarkeit und normale Sichtbarkeit, muss pseudonyme Nutzung als Regelfall offenbleiben.[4] Staatlich verknüpfte Identitätsprüfung, Klarnamenzwang und routinemäßige personenbezogene Querverknüpfung dürfen nicht zur normalen Voraussetzung solcher Teilnahme werden.[5]

Wer allgemeine digitale Diskursräume an staatlich verknüpfte Identität bindet, verschiebt die Architektur von kontobezogener Moderation zu personenbezogener Herrschaft. Aus Moderation werden Personenanker, aus Sichtbarkeitssteuerung wird Exklusionsmacht, aus Missbrauchsabwehr wird die technische Möglichkeit dauerhafter digitaler Ächtung.[6] Das steht in tiefer Spannung zu Meinungsfreiheit, Privatheit, Datensparsamkeit, Verhältnismäßigkeit und effektiven Rechtsbehelfen.[7]

Wir verlangen deshalb einen engen, aber klaren Minimalstandard:

(1) Darf die ordentliche Teilnahme an allgemeinen digitalen Diskursplattformen nicht von staatlich verknüpfter Identifikation, Klarnamenzwang oder biometrischer Personenverifikation abhängig gemacht werden.[8]
(2) Muss pseudonyme Nutzung der Regelfall bleiben. Freiwillige Verifikation für eng begrenzte Zusatzfunktionen mag zulässig sein, darf aber nicht in einen faktischen Teilnahmezwang umschlagen.[9]

---

1 European Board for Digital Services: Das Europäische Gremium für digitale Dienste ist das im DSA eingerichtete Kooperations- und Beratungsgremium. Es setzt sich aus den nationalen Digital Services Coordinators zusammen und wird von der Europäischen Kommission geleitet. Offizielle Seite: https://digital-strategy.ec.europa.eu/en/policies/dsa-board

2 Digital Services Coordinators: Die nationalen Digital Services Coordinators sind die je Mitgliedstaat benannten Behörden für Anwendung, Überwachung und Durchsetzung des DSA. Offizielle Übersichtsseite: https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs

3 Datenschutzaufsichtsbehörden: Gemeint sind die jeweils zuständigen nationalen Datenschutzbehörden; eine offizielle Übersicht ihrer Mitglieder und Webseiten führt das European Data Protection Board. Offizielle Seite: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en

4 Ordentliche Teilnahme: Gemeint ist absichtlich nicht jede denkbare Spezialfunktion eines Dienstes, sondern der Kern allgemeiner digitaler Rede, also insbesondere Posten, Antworten, Folgen, Auffindbarkeit und normale Sichtbarkeit im Diskursraum.

5 Staatlich verknüpfte Identitätsprüfung: Gemeint sind Modelle, bei denen die gewöhnliche Teilnahme an den digitalen Diskurs an einen staatlich rückführbaren Personenanker, an amtliche Ausweisdaten oder an gleichwertige, backend-seitig personenbezogen korrelierbare Verifikationsmechanismen gebunden wird. Dies ist enger als jede beliebige Form von Authentifizierung.

6 Personenanker: Ein stabiler backend-seitiger Identifikator, Hash, Token, UUID oder eine äquivalente Verknüpfungslogik, die aus Account bezogener Moderation eine personenbezogene Ausschlussarchitektur machen kann.

7 Rechtsrahmen: Der engste belastbare Unterbau liegt in der Kombination aus Grundrechten, Datenschutz und Verfahrensschutz. Relevante Anknüpfungspunkte sind insbesondere die EU-Grundrechtecharta sowie der DSA als europäischer Verfahrens- und Transparenzrahmen. Offizielle Texte:
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065

8 Biometrische Personenverifikation: Gemeint sind insbesondere Gesichts- oder andere biometrische Prüfverfahren, soweit sie als Normalvoraussetzung für gewöhnliche Teilnahme am allgemeinen Diskurs eingesetzt würden.

9 Pseudonyme Nutzung als Regelfall: Der Punkt ist nicht, jede Verifikation überall zu verbieten, sondern den öffentlichen oder halböffentlichen Diskursraum gegen die Normalisierung personenverknüpfter Zugangsgates zu sichern.

(3) Dürfen Identitätsdaten oder daraus abgeleitete stabile Personenanker nicht als normales Instrument für kontenübergreifende Moderation, Reichweitensteuerung, Re-Registration-Sperren oder Vertrauenshierarchien im allgemeinen Diskurs dienen.[10] Eng begrenzte Ausnahmen kommen nur bei konkret bestimmten, schweren und rechtlich kontrollierten Konstellationen in Betracht, und nur so weit technisch datensparsam und verhältnismäßig umsetzbar.[11]

(4) Sind Verifikation und Moderation technisch und organisatorisch strikt zu trennen. Was für eng umrissene Nachweiszwecke erhoben wird, darf nicht in ein allgemeines Moderations-, Sichtbarkeits- oder Sanktionsprofil zurückfließen.[12]

(5) Müssen Sichtbarkeits- und Ausschlussentscheidungen begründet, dokumentiert und anfechtbar sein. De-indexierung, Reichweitenreduktion, Verbergungslabels, Kontoeinschränkungen und Suspendierungen dürfen nicht als stille Architekturentscheidungen im Backend verschwinden.[13]

(6) Müssen Datensparsamkeit, begrenzte Speicherung und Löschung ausdrücklich gelten. Identitäts- oder Verknüpfungsdaten dürfen nicht auf Vorrat für künftige Governancezwecke vorgehalten werden. Wo eng begrenzte Aufbewahrung rechtlich erforderlich ist, muss sie spezifisch, zeitlich begrenzt, technisch separiert und überprüfbar sein.[14]

(7) Dürfen Portabilität und Exit nicht ins Leere laufen. Wo Protokolle oder Dienste Kontomigration und technischen Wechsel erlauben, dürfen Identitäts- und Moderationssysteme diese Möglichkeiten nicht faktisch entwerten, indem Sichtbarkeit oder Teilnahme an fortwirkende Personenanker gebunden werden.[15]

Missbrauchsabwehr, Minderjährigen Schutz und Plattformintegrität sind legitime Ziele. Sie rechtfertigen jedoch nicht die Normalisierung personenbezogener Zugangsgates für gewöhnliche Rede. Funktionsspezifische, datensparsame und verhältnismäßige Sicherungen sind möglich. Allgemeine digitale Diskursräume dürfen nicht in Infrastrukturen überführt werden, in denen Identität, Sichtbarkeit und Ausschluss auf Personenebene zusammenfallen.[16]

Wir fordern Betreiber, Aufsichtsbehörden und zuständige europäische Stellen auf, diesen Minimalstandard als verbindliche Leitlinie für allgemeine digitale Diskursplattformen anzuerkennen und umzusetzen.

---

10 Kontenübergreifende Moderation: Gemeint ist nicht gewöhnliche Moderation eines einzelnen Kontos, sondern die Übertragung eines Moderations- oder Ausschlussstatus auf weitere Konten derselben Person auf Grundlage eines stabilen Personenankers.

11 Rechtlich kontrollierte Konstellationen: Gemeint sind keine offenen Sicherheitsfloskeln, sondern eng begrenzte Ausnahmen mit klarer gesetzlicher oder gerichtlicher Grundlage, transparenter Zweckbindung und überprüfbarer Verhältnismäßigkeit.

12 Trennung von Verifikation und Moderation: Wo Nachweise für eng umrissene Zwecke überhaupt erforderlich sind, dürfen sie nicht in allgemeine Moderations- oder Sichtbarkeitsprofile zurückfließen.

13 Begründet, dokumentiert, anfechtbar: Der DSA sieht für bestimmte Moderationsentscheidungen Begründungs- und Beschwerdemechanismen vor. Die Petition verdichtet dies zur Forderung, dass auch De-indexierung und andere faktische Sichtbarkeitseingriffe nicht still im Backend verschwinden dürfen. Offizielle DSA-Seite: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

14 Datensparsamkeit und begrenzte Speicherung: Der datenschutzrechtliche Kern liegt darin, dass Identitäts- und Verknüpfungsdaten nicht für künftige, unbestimmte Governancezwecke auf Vorrat gehalten werden sollen.

15 Portabilität und Exit: Gerade in offenen oder offenen-nahen Protokollumgebungen darf Migration nicht dadurch ins Leere laufen, dass ein fortwirkender Personenanker Sichtbarkeit oder Teilnahme praktisch überall wieder einfängt.

16 Legitime Ziele, aber keine Blanket-Gates: Der Entwurf bestreitet weder Missbrauchsabwehr noch Minderjährigen Schutz. Er wendet sich gegen die Verallgemeinerung dieser Ziele in Richtung Blanket-artiger, personengebundener Zugangsgates für gewöhnliche Rede.